The Termite and the Tower: Goodstein sequences and provability in PA

Will Sladek *

May 17, 2007

Abstract

We discuss Goodstein's Theorem, a true finitary statement that can only be proven by infinitary means. We assume very little knowledge of logic and provide the necessary background to understand both Goodstein's Theorem and, at a high level, how to show that a statement is true but not provable inside a given set of axioms.

1 Introduction

This article presents Goodstein's Theorem, a theorem that makes no reference whatsoever to any notion of infinity, but whose proof must necessarily contain a reference to infinite sets. We do not give a complete proof that Goodstein's Theorem relies inescapably on infinite sets (see [2] for a complete proof), but rather we sketch the high level approach and try to provide the background to understand the importance of the result. In the process, we introduce the reader to some important tools of modern logic—the ordinal numbers, a fundamental construct used heavily by logicians, and the Wainer Hierarchy of functions, a classification of the growth rates of functions from $\mathbb{N}$ to $\mathbb{N}$.

Less than a century ago, many mathematicians did not accept that a mathematical statement could be unprovable. In his 1931 book *Lattice Theory*, Garret Birkoff stated:

> [The existence of undecidable propositions] depends . . . on prescribing all admissible methods of proof . . . [and so] should be viewed with deep skepticism. [4]

The previous quotation was prompted by Kurt Gödel's publication of his now infamous Incompleteness Theorem [9]. In it, he showed that any set of axioms powerful enough to construct the Natural Numbers could inevitably express statements that could not be proven from said axioms. But the statements

*The author would like to extend his sincerest thanks to Andrés Caicedo. His innumerable suggestions and corrections played a crucial role in the development of this article.

formulated by Gödel were contrived—coding statements about first-order logic using the tools of number theory, rather than statements of the kind a number theorist would be expected to consider—leading to speculation that Gödel's Incompleteness Theorem would not have meaningful implications to practical mathematics [24]. However, in 1977, Paris and Harrington [18] showed that a very natural variation of Ramsey's Theorem was true, but not provable from the axioms of Peano arithmetic (PA), the formal system corresponding to number theory. Similarly, in 1982, Kirby and Paris [22, 13] showed that Goodstein's Theorem, which Goodstein originally proved in 1944, is also unprovable in PA.

In order to rigorously perform mathematics with only finite sets, we need a formalism that characterizes the universe of finite sets. As we will discuss further in Section 6, ZFCfin is the set of axioms that comprises standard mathematics with the Axiom of Infinity ("there exists an infinite set") replaced with the axiom "all sets are finite." ZFCfin captures the intuitive notion of finitary mathematics, which we reinforce with the following definition.

Definition 1. Finitary mathematics is mathematics that can be carried out in ZFCfin.

Mathematicians often wish to talk about whether or not an algorithm exists by which a computer (or very patient person) could compute the value of a function. Alan Turing formalized this notion of computability by constructing a simple, theoretical "computer" known as a Turing Machine. There is a significant body of evidence showing that the formal notion of Turing machine captures the informal notion of a finite algorithm. For a more in-depth discussion about Turing machines and their role in studying algorithms; see [5, 23].

Definition 2. A **total function** is a function that is defined on every member of the domain.

Traditionally, total functions and functions are the same thing, but the word total is used to separate them from partial functions, which are only defined on part of their domain.

Definition 3. A function (or partial function) $h : \mathbb{N}^k \to \mathbb{N}$ is **recursive** (or computable) if and only if there is a Turing machine that, with input an arbitrary $\vec{n} \in \mathbb{N}^k$, halts precisely when $h(\vec{n})$ is defined, in which case the machine outputs $h(\vec{n})$.

Since a (partial) recursive function is the output of a finite algorithm, for a given set of inputs, we do not know *a priori* whether or not the algorithm ever stops, yielding the value of the function on these inputs. In particular, when we mention that a recursive function f is "provably total," from certain axioms, we mean to emphasize that the statement $\forall \vec{n} \exists m (f(\vec{n}) = m)$ (equivalently, "the Turing machine that calculates f stops on all inputs") can be proven from the axioms.

At this stage, it is reasonable to wonder how we can show that a completely finitary theorem cannot be proven in finitary terms. How can we say with certainty that no one in the universe is clever enough to circumvent the reference to

infinity? As we mentioned earlier, the axioms of ZFCfin completely characterize finite mathematics. However, ZFCfin is not the natural setting for the results of this article. Instead, we frame our arguments within the axioms of PA, which, in a strong sense to be made precise in Section 6, prove the same statements as ZFCfin. In 1952, Georg Kreisel gave an upper bound on the growth rate of any recursive function that is provably total in PA [14]. Thus, to show that a theorem is unprovable in PA, we first use the theorem to prove in (PA + theorem) that some fast-growing recursive function is total. Then, we just need to show that the fast-growing function grows too quickly for PA. With this in mind, we now go through the definition of Goodstein Sequences and then build some of the tools that we need to prove Goodstein's Theorem and understand why its proof cannot be completed in PA.

2 Goodstein Sequences

Goodstein sequences were first invented by Rueben Louis Goodstein. He presented them in his 1944 paper *On the Restricted Ordinal Theorem* [10], along with Goodstein's Theorem, which remarkably claims that every Goodstein sequence is eventually zero. In order to define Goodstein Sequences, we must first begin by recalling the definition of the base b representation of a number.

Definition 4. For $b \geq 2$, the **base** b **representation** of $n \in \mathbb{N}$ is

$$n = c_0 b^k + c_1 b^{k-1} + \cdots + c_{k-1} b + c_k$$

where $c_0 > 0$ and $0 \leq c_i < b$ for all $0 \leq i \leq k$. Note that the base b representation of a number is unique.

Example 1. We compute the base 2 representation of 266:

$$266 = 2^8 + 2^3 + 2.$$

Definition 5. The **complete base** b **representation** of $n \in \mathbb{N}$ is obtained by computing the base b representation of n, and then replacing every number m in the base b representation by its own base b representation, that is, the representation of m. Repeat this process until all numbers in the current representation are no larger than b.

Example 2. We continue with the example of 266. The complete base 2 representation of 266 is

$$266 = 2^8 + 2^3 + 2 = 2^{2^3} + 2^{2+1} + 2 = 2^{2^{2+1}} + 2^{2+1} + 2.$$

We need one final piece of machinery to define Goodstein Sequences—the change of base function.

Definition 6. Define the **change of base function** $R_b : \mathbb{N} \to \mathbb{N}$ to be the function that takes a natural number n, and then replaces every b with $b+1$ in the complete base b representation of n.

Example 3. To illustrate R_b, we calculate $R_2(266)$.

$$R_2(266) = R_2(2^{2^{2+1}} + 2^{2+1} + 2) = 3^{3^{3+1}} + 3^{3+1} + 3.$$

Note how quickly the sequence $R_b(n)$, $R_{b+1}(R_b(n)), \ldots$ grows—faster than exponentially for most n. On the other hand, notice that for any n, if $b > n$, $R_b(n) = n$.

Definition 7. The **Goodstein Sequence** beginning with n, $(n)_k$, is defined by:

$$\begin{array}{rcl} (n)_0 & = & n \\ (n)_1 & = & R_2(n) - 1 \\ (n)_2 & = & R_3((n)_1) - 1 \\ & \vdots & \\ (n)_{k+1} & = & \begin{cases} R_{k+2}((n)_k) - 1 & \text{if} \quad (n)_k > 0 \\ 0 & \text{if} \quad (n)_k = 0. \end{cases} \end{array}$$

Example 4. For small n, it is easy to see that $(n)_k$ is eventually 0.

$$\begin{array}{rcl} (1)_0 & = & 1 \\ (1)_1 & = & R_2(1) - 1 \quad = \quad 0 \end{array}$$

$$\begin{array}{rcl} (2)_0 & = & 2 \\ (2)_1 & = & R_2(2) - 1 \quad = \quad 3 - 1 = 2 \\ (2)_2 & = & R_3(2) - 1 \quad = \quad 2 - 1 = 1 \\ (2)_3 & = & R_4(1) - 1 \quad = \quad 1 - 1 = 0 \end{array}$$

$$\begin{array}{rcl} (3)_0 & = & 3 \\ (3)_1 & = & R_2(3) - 1 \quad = \quad 3 + 1 - 1 = 3 \\ (3)_2 & = & R_3(3) - 1 \quad = \quad 3 \\ (3)_3 & = & R_4(3) - 1 \quad = \quad 2 \\ (3)_4 & = & R_5(2) - 1 \quad = \quad 1 \\ (3)_5 & = & R_6(1) - 1 \quad = \quad 0. \end{array}$$

However, for $n > 3$, the convergence is not nearly as quick. As we compute the first few values of the Goodstein Sequence beginning with 4, pay attention to the "structure" of b representations—at each stage, subtracting one slowly chips away at the rightmost tower of exponents in the complete representation of numbers along the sequence, but no new towers are ever made that are as large as the ones that are destroyed. This observation is the key to the proof of

Goodstein's Theorem.

$$\begin{array}{rcllcl}
(4)_0 &=& 4 & & & \\
(4)_1 &=& R_2(4)-1 &=& 3^3-1 &=& 26 \\
(4)_2 &=& R_3(26)-1 &=& 2\cdot 4^2+2\cdot 4+2-1 &=& 41 \\
(4)_3 &=& R_4(41)-1 &=& 2\cdot 5^2+2\cdot 5+1-1 &=& 60 \\
(4)_4 &=& R_5(60)-1 &=& 2\cdot 6^2+2\cdot 6-1 &=& 83 \\
(4)_5 &=& R_6(83)-1 &=& 2\cdot 7^2+7+5-1 &=& 109 \\
(4)_6 &=& R_7(109)-1 &=& 2\cdot 8^2+8+4-1 &=& 139 \\
&\vdots & & & & &
\end{array}$$

The changes to the structure of the complete base b representation of 266 are even more evident. Later, we use the ordinal numbers to formalize this concept of structure change into a proof of Goodstein's Theorem.

$$\begin{array}{rcll}
(266)_0 &=& 2^{2^{2+1}}+2^{2+1}+2 &= 266 \\
(266)_1 &=& 3^{3^{3+1}}+3^{3+1}+3-1 &\approx 4.4\times 10^{38} \\
(266)_2 &=& 4^{4^{4+1}}+4^{4+1}+2-1 &\approx 3.2\times 10^{616} \\
(266)_3 &=& 5^{5^{5+1}}+5^{5+1}+1-1 &\approx 2.5\times 10^{10921} \\
(266)_4 &=& 6^{6^{6+1}}+6^{6+1}-1 &\approx 3.5\times 10^{217832} \\
(266)_5 &=& 7^{7^{7+1}}+5\cdot 7^7+5\cdot 7^5+5\cdot 7^4+ & \\
& & 5\cdot 7^3+5\cdot 7^2+5\cdot 7+5-1 &\approx 1.1\times 10^{4871822} \\
(266)_6 &=& 8^{8^{8+1}}+5\cdot 8^8+5\cdot 8^5+5\cdot 8^4+ & \\
& & 5\cdot 8^3+5\cdot 8^2+5\cdot 8+4-1 &\approx 1.7\times 10^{121210686} \\
&\vdots & &
\end{array}$$

Another point to note in the previous examples is the number of iterations that each Goodstein sequence takes before it reaches 0. For the first three Goodstein sequences, this value is tractable. However, at the fourth it takes a wild leap upwards. The number of iterations before $(266)_k = 0$ is unfathomably large.

Definition 8. The **Goodstein Function** $\mathcal{G} : \mathbb{N} \to \mathbb{N}$ is defined to be $k+1$ where k is the smallest number for which $(n)_k = 0$.

Example 5. Here are the first few values of the function $\mathcal{G}$:

$$\begin{array}{rcl}
\mathcal{G}(1) &=& 2 \\
\mathcal{G}(2) &=& 4 \\
\mathcal{G}(3) &=& 6 \\
\mathcal{G}(4) &=& 3\cdot 2^{402653211}-2.
\end{array}$$

Pay particular attention to the massive jump between $\mathcal{G}(3)$ and $\mathcal{G}(4)$. As we mentioned in the introduction, the rate at which the Goodstein Function grows

will be the key to showing that Goodstein's Theorem is outside the grasp of PA. In order to both prove Goodstein's Theorem and to formalize the notion of function growth rate, we need to extend the natural numbers to include infinite numbers. The class of these extended numbers is known as the ordinals.

3 Ordinals

Definition 9. An ordering $<$ on a set X is a **well-ordering** if and only if for any non-empty $Y \subset X$, there exists $m \in Y$ such that for all $y \in Y$ with $y \neq m$, $m < y$ (i.e. Y has a least element with respect to $<$).

Definition 10. Ordered sets $(X, >_X)$ and $(Y, >_Y)$ have the same **order type** if they are order isomorphic, i.e. there exists an order preserving bijection between X and Y.

The **ordinals** can be considered as a transfinite extension of the natural numbers and were originally introduced by Cantor [3] in 1897 as equivalence classes of well-ordered sets modulo order type. Later, von Neumann [25] proposed a canonical way of choosing representatives of each equivalence class. This is how we build the ordinals; we begin by constructing the natural numbers as sets. First, we define 0 as the empty set and then each integer as the set of all integers below it:

Definition 11.

$$\begin{aligned}
0 &= \emptyset \\
1 &= \{0\} = \{\emptyset\} \\
2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\
3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots \\
n &= \{0, \ldots, n-1\} \\
&\vdots \\
\mathbb{N} &= \{0, 1, \ldots\}.
\end{aligned}$$

Now it is easy to define the ordering on $\mathbb{N}$.

Definition 12. If n, $m \in \mathbb{N}$, then say $n < m$ if and only if $n \in m$.

In defining $\mathbb{N}$, we have already implicitly used the notion of the successor of a natural number. By formalizing this notion, we can easily define the standard arithmetic operations on $\mathbb{N}$.

Definition 13. The **successor** of $n \in \mathbb{N}$ is $S(n) = n \cup \{n\} = \{0, \ldots, n\}$.

In standard arithmetic notation, $S(n)$ is merely $n + 1$.

Definition 14. $n + m = \underbrace{S \ldots S}_{m \text{ times}}(n)$.

Note the order of the addition. In this case, apply the successor operation to n, not to m. Once we jump to infinite numbers, this distinction will be important because addition will not be commutative.

We make our first steps away from the finite by creating a new number, ω, which is greater than every natural number. Given our definition of $<$, there is a natural way of defining the *first* such number—the smallest set that contains every natural number. We then proceed as we did with the natural numbers. Note that our definition of $<$ as $\in$ holds and that our definition of S is naturally extended to the infinite ordinals.

Definition 15.

$$\begin{array}{rcll}
\omega & = & \{0,1,\ldots\} & \\
\omega+1 & = & S(\omega) & = \{0,1,\ldots,\omega\} \\
\omega+2 & = & S(\omega+1) & = \{0,1,\ldots,\omega,\omega+1\} \\
 & \vdots & & \\
\omega+n & = & \underbrace{S\ldots S}_{n \text{ times}}(\omega) & = \{0,1,\ldots,\omega,\ldots,\omega+(n-1)\} \\
 & \vdots & & \\
\omega\cdot 2 & = & \omega+\omega & = \{0,1,\ldots,\omega,\omega+1,\ldots\}.
\end{array}$$

Pictorially, at this stage, we have two copies of the natural numbers appended next to each other:

$$\omega\cdot 2 = \underbrace{---------}_{\omega}\ \underbrace{---------}_{\omega}.$$

It is clearest to continue extending the ordinal numbers pictorially. Bear in mind that formally, each ordinal is defined to be the set containing all of the ordinals that came before it in the construction.

$$\begin{array}{rcl}
\omega\cdot 3 & = & \underbrace{---------}_{\omega}\ \underbrace{---------}_{\omega}\ \underbrace{---------}_{\omega} \\
 & \vdots & \\
\omega\cdot n & = & \underbrace{---------\ ---------\ \cdots\ ---------}_{n \text{ times}} \\
 & \vdots & \\
\omega^2 & = & \omega\cdot\omega = \underbrace{------\ \ ------\ \ ------\cdots}_{\omega \text{ times}} \\
 & \vdots & \\
\omega^3 & = & \omega^2\cdot\omega = \underbrace{\underbrace{---\ \ ---\ \cdots}_{\omega \text{ times}}\ \ \underbrace{---\ \ ---\ \cdots}_{\omega \text{ times}}\ \cdots}_{\omega \text{ times}} \\
 & \vdots &
\end{array}$$

$$
\begin{aligned}
\omega^n &= \omega^{n-1}\omega \\
&\vdots \\
\omega^\omega &= \underbrace{\omega \cdot \omega \cdot \ldots}_{\omega \text{ times}} \\
&\vdots \\
\omega^{\omega^2} &= \underbrace{\omega^\omega \cdot \omega^\omega \cdot \ldots}_{\omega \text{ times}} \\
&\vdots \\
\omega^{\omega^\omega} &= \omega \cdot \omega^\omega \cdot \omega^{\omega^2} \cdot \omega^{\omega^3} \cdot \ldots \\
&\vdots \\
\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}\Big\}{\scriptstyle n+1 \text{ times}} &= \omega^{\cdot^{\cdot^{\cdot^{\omega^0}}}}\Big\}{\scriptstyle n \text{ times}} \cdot \omega^{\cdot^{\cdot^{\cdot^{\omega^1}}}}\Big\}{\scriptstyle n \text{ times}} \cdot \omega^{\cdot^{\cdot^{\omega^2}}}\Big\}{\scriptstyle n \text{ times}} \cdot \ldots \\
&\vdots \\
\epsilon_0 &= \omega^{\cdot^{\cdot^{\cdot}}}\Big\}{\scriptstyle \omega \text{ times}}.
\end{aligned}
$$

(Note that our intuitive use of the addition and multiplication symbols is actually the standard use of these symbols as operations on order types. See [20] for details on how these operations can be formalized.)

From here, we can continue this process to define $\epsilon_0 + 1$, $\epsilon_0 + n$, $\epsilon_0^{\epsilon_0}$, etc. We do not explicitly need any ordinals larger than ϵ_0 for the purposes of this paper. However, they are a fundamental tool that is interesting to explore more deeply for their own sake. We now take a moment to highlight some of the fundamental properties of the ordinals.

Fact 1 ([25])**.** *Every ordinal, and in general every set of ordinals, is well-ordered.*

In fact, since our definition of ordinals is equivalent to Cantor's definition in terms of order types of well-ordered sets, then a stronger result holds: every well-ordered set is order isomorphic to precisely one ordinal.

Definition 16. An ordinal ϕ is a **limit ordinal** (or just a limit) if for any ordinal $\psi < \phi$, there are infinitely many ordinals τ (equivalently, at least one) for which $\psi < \tau < \phi$.

Definition 17. An ordinal ϕ is a **successor ordinal** (or just a successor) if there exists an ordinal ψ such that $\phi = S(\psi) = \psi + 1$.

The following theorem is immediate from the definitions:

Theorem 2. *An ordinal ϕ is precisely one of the following:* 0*, a successor, or a limit.*

A crucial fact is that we can extend induction from $\mathbb{N}$ to the ordinals to obtain *transfinite induction*. This notion is formalized in the following theorem:

Theorem 3 (Transfinite induction)**.** *Let α be an ordinal and $P(\alpha)$ be some statement. Then if for every α, $P(\alpha)$ follows from the fact that $P(\beta)$ holds for every $\beta < \alpha$, then $P(\alpha)$ is true for all ordinals α. Formally:*

$$\forall\alpha\,[\forall\beta\,(\beta < \alpha \to P(\beta)) \to P(\alpha)] \Longrightarrow \forall\alpha\,P(\alpha).$$

Proof. Suppose that the theorem is false, and we have an ordinal α for which the statement $P(\alpha)$ is false, even though the hypothesis of the theorem holds. Since the ordinals are well-ordered, there is a least ordinal γ for which $P(\gamma)$ is false. However, for all $\beta < \gamma$, $P(\beta)$ holds (by minimality of γ), and therefore $P(\gamma)$ holds as well (by hypothesis), so we have a contradiction. □

In practice, since there are precisely three types of ordinals, we prove that the hypothesis of Theorem 3 holds by proving the following:

1. $P(0)$ is true.
2. If λ is a limit, then $P(\lambda)$ follows from the assumption that $P(\beta)$ holds for all $\beta < \lambda$.
3. $P(\alpha + 1)$ follows from the assumption $P(\alpha)$ holds (or, as in the case of *strong* induction on $\mathbb{N}$, from the assumption that $P(\alpha)$ and $P(\beta)$ hold for all $\beta < \alpha$).

We extensively use transfinite induction in the next section.

Theorem 4. *There is no infinite, strictly decreasing sequence of ordinals.*

Proof. Otherwise, its range would be a non-empty set of ordinals without a first element. □

4 The Hierarchy of Fast Growing Functions

We also need to develop a classification of the rate of growth of functions on $\mathbb{N}$ in order to explore the boundaries of finitary mathematics. The hierarchy that we present here is due to Stanley Wainer and M. Löb [22], [26]. The zeroth and first levels of the hierarchy will be functions that increase linearly. From there, we repeatedly apply the linear functions to themselves to obtain exponential functions, then towers of exponents, next towers of towers of ... towers of exponents, and we blast off from there.

Definition 18. The **nth-iteration** of a function h is $h^n = \underbrace{h \circ \cdots \circ h}_{n \text{ times}}$ where $\circ$ denotes function composition.

Example 6.

$$\begin{array}{rcll}
f_0(n) & = & n+1 & \\
f_1(n) & = & f_0^n(n) & = f_0^{n-1}(n+1) = f_0^{n-2}(n+1+1) = \cdots = 2n \\
f_2(n) & = & f_1^n(n) & = 2^n \cdot n > 2^n \\
f_3(n) & = & f_2^n(n) & > 2^{\overset{\overset{2^n}{\cdot^{\cdot^{\cdot}}}}{\left.\right\}n \text{ times}}} \\
f_4(n) & = & f_3^n(n) & > f_3^{n-1}\left(2^{\overset{\overset{2^n}{\cdot^{\cdot^{\cdot}}}}{\left.\right\}n \text{ times}}}\right) \\
 & \vdots & & \\
f_{m+1}(n) & = & f_m^n(n) & \\
 & \vdots & & \\
f_\omega(n) & = & f_n(n) & \\
f_{\omega+1}(n) & = & f_\omega^n(n) & \\
 & \vdots & &
\end{array}$$

To formally define the hierarchy for limit ordinal subscripts, we need to define a representation of the ordinals that is due to Cantor.

Definition 19. For an ordinal $\alpha < \epsilon_0$, the **Cantor Normal Form** (CNF) of α is the base ω representation of the ordinal. Explicitly, it is

$$\alpha = \omega^{\beta_0} \cdot n_0 + \omega^{\beta_1} \cdot n_1 + \cdots + \omega^{\beta_k} \cdot n_k$$

where $\alpha > \beta_0 > \beta_1 > \cdots > \beta_k$ are ordinals and each $n_i \in \mathbb{N}$, $n_i > 0$.

Fact 5. *The Cantor Normal Form of an ordinal is unique.*

Fact 6. *An ordinal α is a limit if and only if $\beta_k > 0$.*

Corollary 7 ([12])**.** *For every ordinal $0 < \alpha < \epsilon_0$, there is a unique $\beta < \alpha$ such that $\alpha = \omega^\delta(\beta + 1)$, where δ is β_k from the CNF of α.*

Definition 20. For a limit ordinal $\alpha < \epsilon_0$ with $\alpha = \omega^\gamma(\beta+1)$, we define the increasing sequence $d_i[\alpha] \to \alpha$ by induction.

$$\begin{array}{rcll}
d_i[\omega^\gamma(\beta+1)] & = & \omega^{\delta+1} \cdot \beta + \omega^\delta \cdot i & \text{if } \gamma = \delta + 1, \\
d_i[\omega^\lambda(\beta+1)] & = & \omega^\lambda \cdot \beta + \omega^{d_i[\lambda]} & \text{if } \gamma = \lambda \text{ is a limit}, \\
d_i[\epsilon_0] & = & \omega^{\overset{\overset{\omega}{\cdot^{\cdot^{\cdot}}}}{\left.\right\}i \text{ times}}}. &
\end{array}$$

Now we can define f_α concretely by transfinite induction.

Definition 21. For $\alpha \leq \epsilon_0$

$$\begin{array}{rcl}
f_0(n) & = & n+1, \\
f_{\alpha+1}(n) & = & \underbrace{f_\alpha \circ \cdots \circ f_\alpha}_{n \text{ times}}(n) = f_\alpha^n(n), \\
f_\alpha(n) & = & f_{d_n[\alpha]}(n) \text{ if } \alpha \text{ is a limit.}
\end{array}$$

Definition 22. If $f, g : \mathbb{N} \to \mathbb{N}$, then f **dominates** g if there exists an $N \in \mathbb{N}$ such that for all $n > N$, $f(n) > g(n)$.

Fact 8. *Function domination is a transitive relation.*

Theorem 9. *For ordinals α, β, if $\alpha > \beta$, then f_α dominates f_β.*

To rigorously prove Theorem 9, one defines decreasing "walks" (finite sequences) from an ordinal α to $\beta < \alpha$ in terms of the canonical sequences d_n and then uses properties of these walks to place lower bounds on the growth of f_α. Our presentation is a cursory sketch of the complete (and very readable) proof of Ketonen-Solovay [12]. We omit the proofs of many of the intermediate theorems and lemmas, but include enough to see the typical methods used. We first define the walks from a larger ordinal to a smaller.

Previously, we defined $d_n[\alpha]$ only when α was a limit. We now trivially extend this to successor α.

Definition 23. For an ordinal $\alpha = \beta + 1$, $d_n[\alpha] = \beta$.

Definition 24. Let $\alpha < \beta \leq \epsilon_0$. Then $\beta \underset{n}{\to} \alpha$ if for some sequence of ordinals $\gamma_0, \ldots, \gamma_r$ we have $\gamma_0 = \beta$, $\gamma_{i+1} = d_n[\gamma_i]$, for $0 \leq i < r$, and $\gamma_r = \alpha$.

Fact 10. $\underset{n}{\to}$ *is transitive.*

Theorem 11. *Let $\lambda \leq \epsilon_0$ be a limit. Let $i < j \in \mathbb{N}$. Then $d_j[\lambda] \underset{1}{\to} d_i[\lambda]$.*

Proof. See [12], Theorem 2.4. □

Corollary 12. *Let $\beta < \alpha \leq \epsilon_0$ and $n > i$. If $\alpha \underset{i}{\to} \beta$, then $\alpha \underset{n}{\to} \beta$.*

Proof. We induct on α. By transitivity of $\underset{n}{\to}$ we may assume without loss of generality that α is a limit ordinal and $\beta = d_i[\alpha]$. Then by Theorem 11, $d_n[\alpha] \underset{1}{\to} d_i[\alpha] = \beta$. Since $d_n[\alpha] < \alpha$, then by the induction hypothesis, $d_n[\alpha] \underset{n}{\to} \beta$. Thus, by Fact 10, $\alpha \underset{n}{\to} \beta$. □

The following theorem can be proven by induction. Interestingly, it is easier to prove each part of the following proposition simultaneously via induction than to prove each one separately.

Theorem 13. *Let $\alpha \leq \epsilon_0$.*

1. *$f_\alpha(n) > n$.*
2. *If $n > m$, then $f_\alpha(n) > f_\alpha(m)$.*
3. *If $\alpha = \beta + 1$, then $f_\alpha(n) \geq f_\beta(n)$ with strict inequality if $n > 1$.*
4. *If $\alpha \underset{n}{\to} \beta$, then $f_\alpha(n) \geq f_\beta(n)$.*

Proof. See [12], Proposition 2.5. □

Lemma 14. *Let $\alpha > \beta$. Then there is an n such that $\alpha \underset{n}{\rightarrow} \beta$.*

Proof. We induct on α. The theorem is vacuous when $\alpha = 0$ and is easily reduced to the limit case by transitivity when α is a successor. Suppose α is a limit. Since $d_i[\alpha] \rightarrow \alpha$ as $i \rightarrow \infty$, then there is an n_1 so large that $d_{n_1}[\alpha] > \beta$. Thus, by the induction hypothesis, there is an n_2 such that $d_{n_1}[\alpha] \underset{n_2}{\rightarrow} \beta$. By Corollary 12 and transitivity, if we choose $n = \max\{n_1, n_2\}$, $\alpha \underset{n}{\rightarrow} \beta$. □

Lemma 15. *Let $n > 0$ and $\alpha \underset{n}{\rightarrow} \beta$. Then if $\alpha > \beta + 1$, $\alpha \underset{n+1}{\rightarrow} \beta + 1$.*

Proof. See [12], Lemma 2.6.2. □

Lemma 16. *Let $\alpha > \beta$ and $\alpha \underset{n}{\rightarrow} \beta$. Then if $m > n$, $f_\alpha(m) > f_\beta(m)$.*

Proof. We again induct on α. The $\alpha = 0$ case is vacuous. By Lemma 14 and parts (2), (3) of Theorem 13, we know that for $m > n$, $f_{\alpha+1}(m) > f_\alpha(m)$, so it suffices to consider the case when α is a limit. By Lemma 15, $\alpha \underset{m}{\rightarrow} \beta + 1$, so by part (4) of Theorem 13, $f_\alpha(m) \geq f_{\beta+1}(m) > f_\beta(m)$, where the last inequality holds by the induction hypothesis (or by part (3) of Theorem 13). □

Proof of Theorem 9. By Lemma 14, there is an n such that $\alpha \underset{n}{\rightarrow} \beta$. Thus, by Lemma 16, for all $m > n$, $f_\alpha(m) > f_\beta(m)$, which is to say that f_α dominates f_β. □

Using this hierarchy, along with one more useful definition, we can describe very simply the values of the Goodstein Function $\mathcal{G}$. This elegant description was discovered very recently by Andrés Caicedo and has not yet been published.

Definition 25. For $b \geq 2$, the **ω-change of base function**, $R_b^\omega(n)$ is the ordinal that results from taking the complete base b representation of n and replacing every occurrence of b with ω. This will yield an ordinal written in the CNF.

Theorem 17. *Suppose $n = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_{k-1}} + 2^{m_k}$ where $m_1 > m_2 > ... > m_{k-1} > m_k$. Let $\alpha_i = R_2^\omega(m_i)$. Then*

$$\mathcal{G}(n) = f_{\alpha_1}(f_{\alpha_2}(...(f_{\alpha_k}(3))...)) - 2.$$

Example 7.

$$\begin{array}{lcll} \mathcal{G}(1) & = & f_0(3) - 2 & \text{since} \quad 1 = 2^0 \\ \mathcal{G}(2) & = & f_1(3) - 2 & \text{since} \quad 2 = 2^1 \\ \mathcal{G}(3) & = & f_1(f_0(3)) - 2 & \text{since} \quad 3 = 2^1 + 2^0 \\ \mathcal{G}(4) & = & f_\omega(3) - 2 & \text{since} \quad 4 = 2^2 \\ \mathcal{G}(5) & = & f_\omega(f_0(3)) - 2 & \text{since} \quad 4 = 2^2 + 2^0. \end{array}$$

Likewise,

$$\mathcal{G}(266) = f_{\omega^{\omega+1}}(f_{\omega+1}(f_1(3))) - 2$$

because

$$266 = 2^{2^{2+1}} + 2^{2+1} + 2 = 2^{2^{2+1}} + 2^{2+1} + 2^1.$$

It is important to realize that all of the functions f_α that we have defined so far are recursive functions from $\mathbb{N}$ to $\mathbb{N}$, as for each of them there is an easy algorithm to compute their values, following α down to smaller ordinals using the sequence $d_i[\alpha]$. Even though we have employed transfinite induction on infinite ordinals in classifying the functions, a Turing Machine set to compute any value of any of the functions would eventually (given inexhaustible resources) complete its task in a finite amount of time.

We could continue to define recursive f_α for $\alpha > \epsilon_0$ as long as we have a well-defined, recursive method for choosing the sequence $d_i[\alpha]$. This opens the door to the topic of ordinal notations. (For a primer on the subject, see [17].) Eventually, it must become impossible to choose $d_i[\alpha]$ in a recursive fashion because there are only countably many recursive functions while there are ordinals of all cardinalities.

Thus, there are only countably many "recursive ordinals." The first non-recursive ordinal is denoted ω_1^{CK} (CK for Church-Kleene; see [21]). The question of how far the hierarchy can be defined (below ω_1^{CK} of course) before Theorem 9 fails is very much open.

While defining recursive functions in terms of Turing Machines captures the intuitive notion of algorithmically computable, we can define the class of recursive (partial) functions more explicitly using induction.

Definition 26. A (partial) function $h : \mathbb{N}^k \to \mathbb{N}$ is **order** 0 **recursive** if it is one of the following:

1. the constant 0 function,
2. the successor function $S : \mathbb{N} \to \mathbb{N}$, $S(n) = n + 1$,
3. any of the projection functions $p_i : \mathbb{N}^k \to \mathbb{N}$, $p_i(n_1, \ldots, n_k) = n_i$.

A (partial) function $h : \mathbb{N}^k \to \mathbb{N}$ is **order** $n + 1$ **recursive** if it can be formed from order at-most-n recursive functions by applying one of the following operations:

1. (composition) $h(\vec{n}) = f(g_1(n_1), \ldots, g_k(n_k))$,
2. (primitive recursion) $h(n, 0) = f(n)$, $h(n + 1, m) = g(n, m, h(n, m))$,
3. (μ operator) $\mu m(f(m, \vec{n}) =$ "least m for which $g(m, \vec{n}) = 0$").

A (partial) function $h : \mathbb{N}^k \to \mathbb{N}$ is **recursive** if it is order n recursive for some $n \in \mathbb{N}$.

This definition of recursive functions is equivalent to the definition in terms of Turing Machines [5]. The key is that this definition provides a means for inducting over the recursive functions, which leads to the next theorem that combines results of Gödel [9] and the Davis-Putnam-Robinson-Matiyasevich theorem on the unsolvability of Hilbert's tenth problem.

Theorem 18 ([11])**.** *A (partial) function $h : \mathbb{N}^k \to \mathbb{N}$ is recursive if and only if its graph $\{(\vec{a}, b) : h(\vec{a}) = b\}$ is definable in the language of arithmetic (as described in Section 6) by a formula of the form $\exists x \phi(x)$, where $\phi(x)$ is quantifier free.*

This theorem lets us assign to every recursive function h, a formula $\phi_h(\vec{x}, y)$ that describes the behavior of the function. In particular, it has the following properties (where $T \vdash \phi$ denotes that the formula ϕ is formally provable from the axioms of theory T):

1. For all $\vec{n} \in \mathbb{N}^k$ and $m \in \mathbb{N}$, $h(\vec{n}) = m \iff \text{PA} \vdash \phi_h(\vec{n}, m)$.
2. For all $\vec{n} \in \mathbb{N}^k$ and $m \in \mathbb{N}$, $\text{PA} \vdash \phi_h(\vec{n}, m)$ or $\text{PA} \vdash \neg\phi_h(\vec{n}, m)$.
3. $\text{PA} \vdash \forall \vec{x}, y, z\, \phi_h(\vec{x}, y) \wedge \phi_h(\vec{x}, z) \to y = z$.

Note that property (3) does not mean that h is total, but only that h is at least a partial function. Also, note that the quantifiers in property (2) are not part of the formulas. To say that PA proves that the recursive function h is total means that

$$\text{PA} \vdash \forall \vec{x} \exists y\, \phi_h(\vec{x}, y).$$

If PA proves that a recursive function h is total, then we can make a strong statement about the growth rate of h.

Theorem 19 (Kreisel [14])**.** *If a recursive $f : \mathbb{N} \to \mathbb{N}$ is provably total in PA, then f_α dominates f for some ordinal $\alpha < \epsilon_0$.*

The following theorems are not particularly relevant for this paper but are important facts about the Wainer Hierarchy.

Definition 27. The class of **primitive recursive** functions is the subclass of the recursive (partial) functions that can be constructed without using the μ operator. Notice that all primitive recursive functions are total.

In [11], it is shown that all primitive recursive functions are provably total in PA. One can also see there the following strengthening of Theorem 19:

Fact 20 ([11])**.** *If $h : \mathbb{N} \to \mathbb{N}$ is primitive recursive, then it is dominated by f_n for some finite n.*

Fact 21 ([11])**.** *The Ackermann function grows on the order of f_ω.*

5 Goodstein's Theorem

Theorem 22 (Goodstein [10])**.** *For every $n \in \mathbb{N}$ there is a $K \in \mathbb{N}$, such that for all $k \geq K$, $(n)_k = 0$.*

We immediately depart the finite world of PA by taking advantage of the infinite ordinals. The general method of the proof will be to define for each n, a decreasing sequence of ordinals that bounds $(n)_k$ from above. We do this by taking the complete base b representation at each stage of the Goodstein Sequence and replacing all of the b's by ω. The idea is that by always using a base that is larger than any natural number, the change of base operation will have no effect, but subtracting one will still eventually drive this sequence to 0.

Proof of Theorem 22. We define a decreasing, companion sequence of ordinals that bounds $(n)_k$ from above. Fix an $n \in \mathbb{N}$. For $k \in \mathbb{N}$, let $(n)'_k = R^{\omega}_{k+2}((n)_k)$. Clearly, $(n)'_k \geq (n)_k$ (i.e. $(n)'_k$ bounds $(n)_k$ from above), so it simply remains to show that $(n)'_k$ is decreasing. If $(n_k)' > 0$, then so is $(n)_k$, and $(n)'_{k+1} = R^{\omega}_{k+3}((n)_{k+1}) = R^{\omega}_{k+3}(R_{k+2}((n)_k) - 1) < R^{\omega}_{k+3}(R_{k+2}((n)_k)) = R^{\omega}_{k+2}((n)_k) = (n)'_k$. Hence, $(n)'_k$ is strictly decreasing, unless $(n)'_k = 0$, in which case $(n)'_{\overline{k}} = 0$ for all $\overline{k} > k$. Since there is no infinite, strictly decreasing sequence of ordinals, then $(n)'_k$ is eventually 0. Finally, since $(n)'_k$ bounds $(n)_k$ from above, then $(n)_k$ also must eventually decrease to 0. □

Example 8. To illustrate the argument used to prove Goodstein's Theorem, we calculate some of the values of the companion sequence for $n = 266$. Notice that the change of base operation has no effect on the companion sequence, but that the perpetual subtraction of one in the Goodstein Sequence causes the companion sequence to strictly decrease.

$$\begin{aligned}
(266)'_0 &= \omega^{\omega^{\omega+1}} + \omega^{\omega+1} + \omega \\
(266)'_1 &= \omega^{\omega^{\omega+1}} + \omega^{\omega+1} + 2 \\
(266)'_2 &= \omega^{\omega^{\omega+1}} + \omega^{\omega+1} + 1 \\
(266)'_3 &= \omega^{\omega^{\omega+1}} + \omega^{\omega+1} \\
(266)'_4 &= R^{\omega}_6(6^{6^{6+1}} + 6^{6+1} - 1) = \omega^{\omega^{\omega+1}} + \omega^{\omega} \cdot 5 + \omega^5 \cdot 5 + \cdots + \omega \cdot 5 + 5 \\
(266)'_5 &= \omega^{\omega^{\omega+1}} + \omega^{\omega} \cdot 5 + \omega^5 \cdot 5 + \cdots + \omega \cdot 5 + 4 \\
(266)'_6 &= \omega^{\omega^{\omega+1}} + \omega^{\omega} \cdot 5 + \omega^5 \cdot 5 + \cdots + \omega \cdot 5 + 3 \\
&\vdots
\end{aligned}$$

Corollary 23. *The Goodstein function, $\mathcal{G}$, is recursive. In particular, it is a total function from $\mathbb{N}$ to $\mathbb{N}$.*

Proof. Since we have a proof that every Goodstein Sequence will eventually reach 0, then for any n, we can set a Turing Machine to compute the Goodstein Sequence $(n)_k$ until it reaches 0, and then report the first $K+1$ for which $(n)_K = 0$ (i.e. $\mathcal{G}(n) = K + 1$). Note that this corollary is derived from Goodstein's Theorem by entirely finitary means. □

Theorem 24 (Kirby-Paris [22])**.** *The Goodstein function, $\mathcal{G}$ grows on the order of f_{ϵ_0}.*

Corollary 25. *Goodstein's Theorem is not provable in PA.*

Proof. Assume that Goodstein's Theorem is provable in PA. Then by the proof of Corollary 23, $\mathcal{G}$ is provably total in PA. However, Kreisel's Theorem 19 then implies that $\mathcal{G}$ is dominated by f_α for some $\alpha < \epsilon_0$. This contradicts Theorem 24. Therefore, Goodstein's Theorem is not provable in PA. □

Interestingly, even though PA does not prove that $\mathcal{G}$ is total, by Corollary 23, we know that for every $n \in \mathbb{N}$ there is a straightforward, albeit exceedingly long, proof in PA that $\mathcal{G}(n)$ exists—simply compute all of the nonzero terms of the Goodstein Sequence and count all of them. Thus, for any n,

$$\text{PA} \vdash \exists m(\mathcal{G}(n) = m),$$

but

$$\text{PA} \nvdash \forall n \exists m(\mathcal{G}(n) = m).$$

This concisely illustrates the limitations of PA and the need for more powerful axiomatic systems. We know that a statement is true, but we cannot prove it inside PA; therefore we need a stronger system. These limitations are not unique to PA, however. Friedman has discovered examples of natural, unprovable, true statements in much more powerful systems such as ZFC [6].

It is interesting to consider precisely where in the proof of Goodstein's Theorem we step beyond the boundaries of PA. It is not, *a priori*, obvious that we cannot formalize the towers of ω's within PA. As we mentioned previously, the ordinals can be defined as the order types of well-ordered sets. Since all of the ordinals in our discussion (including ϵ_0) are countable, then to define any of them in PA, we simply define a new ordering of $\mathbb{N}$. In particular, any ordering that can be defined as a recursive binary relation (which includes the order type of ϵ_0) can be defined in PA. However, the key property used in the proof of Goodstein's Theorem was that any ordinal is well-ordered, so to formalize the proof of Goodstein's Theorem in PA, we would need a proof in PA that every ordinal below ϵ_0 is well-ordered, or, equivalently, a proof that ϵ_0 is well-ordered, but such a proof does not exist.

One can consider the equivalent problem of formalizing transfinite induction within PA. Gerhard Gentzen [7, 8] showed that for any $\alpha < \epsilon_0$, transfinite induction of length α is formalizable in PA, but that transfinite induction of length ϵ_0 is not formalizable. This leads to another uniform way (due to Kirby and Paris [13]) to prove, for a fixed n, that $(n)_k$ is eventually 0 (other than merely computing the sequence)—prove that the largest tower of ω's in $(n)_0'$ is well-ordered, and then proceed with the proof that we gave above. We can thus pinpoint ϵ_0 as the limit of PA in the sense that ϵ_0 is the first ordinal that PA cannot prove to be well-ordered.

6 PA's Relation to Finitary Mathematics

The statement that PA coincides with finitary mathematics deserves a bit more explanation. The reader has probably heard of the Zermelo-Frankel (ZF) axioms of set theory. Along with the Axiom of Choice (ZF with Choice is denoted ZFC), these axioms provide the foundation for standard mathematics. Of the nine ZFC axioms, most of them are concerned with building new sets from existing ones. An exception is the Axiom of Infinity, which posits the existence of an infinite set.

Definition 28. ZF is the (first-order) theory in the language $\{\in\}$ given by the following 8 (families of) axioms:

1. (Extensionality): Sets with the same elements are equal.

$$\forall x \forall y \left(\forall z \left(z \in x \leftrightarrow z \in y\right) \leftrightarrow x = y\right).$$

2. (Pairing): For any x and y, $\{x, y\}$ exists.

$$\forall x, y \exists z \left(\forall w \left(w \in z \leftrightarrow (w = x \vee w = y)\right)\right).$$

3. (Comprehension): For each property P and set x, there is a set consisting of precisely the elements of x with the property P. Formally: For each formula $\varphi(w, \vec{y})$:

$$\forall \vec{y} \forall x \exists z \forall w \left(w \in z \leftrightarrow (w \in x \wedge \varphi(w, \vec{y}))\right).$$

   From the axioms of first order logic one can prove the existence of sets. Using comprehension (with $P(x)$ any false property, like $x \neq x$) there is a set with no elements. Using extensionality, this set is unique (the empty set), and we denote it $\emptyset$.

4. (Union): For any family X, $\bigcup_{y \in X} y$ exists:

$$\forall x \exists y \forall z \left(z \in y \leftrightarrow \exists w \left(w \in x \wedge z \in w\right)\right).$$

5. (Power set): For any x, the set $P(x)$ of all subsets of x exists.

$$\forall x \exists y \forall z \left(z \in y \leftrightarrow \forall w \left(w \in z \rightarrow w \in x\right)\right).$$

6. (Foundation): Every nonempty set S has an $\in$-minimal element: a $z \in S$ such that $z \cap S = \emptyset$. It is perhaps better to state this axiom as saying that a version of induction over sets holds: For any formula $\phi(z, \vec{w})$:

$$\forall \vec{w} \left(\forall x \left(\left(\forall y \in x \, \phi(y, \vec{w})\right) \rightarrow \phi(x, \vec{w})\right) \longrightarrow \forall x \, \phi(x, \vec{w})\right).$$

7. (Replacement): If F is a function, then for any x,

$$F[x] = \{F(y) : y \in x\}$$

exists: Formally, for each formula $\varphi(\vec{x}, z, \vec{y})$:

$$\begin{array}{lll} \forall \vec{y} & (& \forall \vec{x}\, \exists^{=1} z\, \varphi(\vec{x}, z, \vec{y}) \longrightarrow \\ & & \forall w \exists v \forall u\, (u \in v \longleftrightarrow \\ & & \exists x_0, \ldots, x_{n-1}\, (\bigwedge_{i<n} x_i \in w \wedge \varphi(\vec{x}, u, \vec{y}))) \ ). \end{array}$$

8. (Infinite) : There is an infinite set. Specifically, we require that there is a set from which ω can be constructed.

$$\exists w\, (\emptyset \in w \wedge \forall y \in w\, (y \cup \{y\} \in w)).$$

We can go on to define ordered pairs: $(a, b) = \{\{a\}, \{a, b\}\}$ and then proceed to define functions and relations as sets of ordered pairs. We can also formally define the natural numbers (as we did in section 3) and then define a set to be finite if and only if it is in bijection with a natural number.

ZFC, the standard formal framework for modern mathematics, is the ZF axioms together with the Axiom of Choice, which asserts that if X is a set of nonempty sets, then there is a function f (called a choice function) that takes each $x \in X$ to an element of x, i.e. $f(x) \in x$.

Obviously, with the Axiom of Infinity, ZFC extends well beyond finitary mathematics. We can easily remedy this situation by replacing the Axiom of Infinity with a new axiom, the Axiom of Finite Sets. This new set of axioms is the natural interpretation of the phrase "finitary mathematics."

Definition 29. ZFCfin is the list of ZFC axioms with the Axiom of Infinity replaced by the axiom "there are no limit ordinals." From this, one can show that all sets are finite as defined above.

We should note that it is not necessary to include the Axiom of Choice in ZFCfin since it can be proven from the "ZFfin" axioms. We include it as an axiom to simplify our presentation.

We can define the **standard model** of ZFCfin by starting with the empty set and using the power set operation to construct the universe of all finite sets.

Definition 30.

$$\begin{array}{rcl} V_0 & = & \emptyset \\ V_1 & = & \{\emptyset\} \\ & \vdots & \\ V_{n+1} & = & P(V_n) \\ & \vdots & \end{array}$$

A straightforward induction shows that each V_n is *transitive* and the sequence is increasing, i.e., for each n, every element of V_n is a *subset* of V_n, and $V_n \in V_{n+1}$.

Definition 31. The **hereditarily finite** sets are the members of

$$HF = \bigcup_{n \in \mathbb{N}} V_n.$$

$(HF, \in)$ satisfies ZFCfin (in symbols, $HF \models$ ZFCfin). This is what we mean by finitary mathematics. One can prove in ZFCfin that sets are precisely the members of HF. Note that when we built the finite ordinals, we were working inside $(HF, \in)$. However, ZFCfin is not a very convenient setting for dealing with fast-growing functions; PA is much more natural. Formally, the language of PA is $\{0, S, +, \times\}$ where S is the successor function $S(n) = n+1$. In this language it is convenient to build functions by iterations of addition and multiplication, so PA is a natural setting for proving independence theorems such as Goodstein's Theorem.

Definition 32. PA is the theory in the language $\{0, S, +, \times\}$ given by the axioms:

1. $\forall x\,(Sx \neq 0)$.
2. $\forall x, y\,(Sx = Sy \to x = y)$.
3. $\forall x\,(x + 0 = x)$.
4. $\forall x, y\,(x + Sy = S(x + y))$.
5. $\forall x\,(x \times 0 = 0)$.
6. $\forall x, y(x \times Sy = (x \times y) + x)$.
7. (Induction): For each formula $\varphi(x, \vec{y})$:

$$\forall \vec{y}\,((\varphi(0, \vec{y}) \wedge \forall x\,(\varphi(x, \vec{y}) \to \varphi(Sx, \vec{y}))) \to \forall x\,\varphi(x, \vec{y})).$$

Fortunately PA and ZFCfin are biinterpretable, which among other things means that any statement provable in ZFCfin is also provable in PA and vice versa. More specifically, we can define a *translation* t of the symbol $\in$ into the language of PA. The translation consists of an arithmetic formula $B(x, y)$, and we translate an arbitrary formula φ about sets into an arithmetic formula φ^t by replacing each instance of $x \in y$ in φ with $B(x, y)$. This translation is defined so that for any ZFCfin axiom φ, its translation, φ^t, is a theorem of PA. Similarly, for every symbol in the language of PA, we define a translation t' into the language of ZFCfin so that if ψ is an axiom of PA, then $\psi^{t'}$ is a theorem of ZFCfin. These translations have the property that if φ is any formula in the language of ZFCfin, then

$$\text{ZFCfin} \vdash \varphi \leftrightarrow (\varphi^t)^{t'}$$

and if ψ is any formula in the language of PA, then

$$\mathrm{PA} \vdash \psi \leftrightarrow (\psi^{t'})^t.$$

Alternatively, we can phrase the translations in terms of *models* of PA and ZFCfin. If $\mathcal{M} \models \mathrm{ZFCfin}$ and $\mathcal{N} \models \mathrm{PA}$, to each we respectively assign $P_{\mathcal{M}} \models \mathrm{PA}$ (defined in terms of t) and $Z_{\mathcal{N}} \models \mathrm{ZFCfin}$ (defined in terms of t') that have the property that

$$Z_{P_{\mathcal{M}}} \cong \mathcal{M} \text{ and } P_{Z_{\mathcal{N}}} \cong \mathcal{N}.$$

Thus, ZFCfin and PA are just two different means of expressing (and proving) the same statements.

We briefly demonstrate how to define the standard models HF and ω within each other. Given the model HF that we defined above, it is easy to define ω because we have already defined the ordinals inside HF. Thus, we just define $+$ and $\times$ to be ordinal addition and ordinal multiplication, and we are done. Defining ZFCfin inside PA is trickier, but not difficult.

Definition 33. Let E be the binary relation on $\mathbb{N} \times \mathbb{N}$ defined by nEm if and only if there is a 1 in the nth place from the right of the binary representation of m.

Example 9. The binary representation of 21 is 10101, so $0E21$, $2E21$, and $4E21$ while $\neg 1E21$.

Theorem 26. $(\omega, E) \cong (HF, \in)$.

Proof. For each n, we construct via induction an isomorphism ϕ_n between $(|V_n|, E)$ and $(V_n, \in)$ so that ϕ_{n+1} extends ϕ_n . For $n = 0$, $\phi_0 = \emptyset$ is the (trivial) empty isomorphism. Suppose we have constructed isomorphisms up to ϕ_n. Notice that $|V_{n+1}| = 2^{|V_n|}$, so if $m < 2^{|V_n|}$, then the base 2 representation of m is the sum of powers 2^k where $k < |V_n|$, namely, precisely those k such that kEm. Therefore, by the induction hypothesis, each $\phi_n(k)$ is defined, so set

$$\phi_{n+1}(m) = \{\phi_n(k) : kEm\}.$$

To see that ϕ_{n+1} is a bijection, notice that any $x \in V_{n+1}$ is a subset of V_n, so $x = \{x_1, \ldots, x_k\}$ where each $x_i \in V_n$; thus, by the induction hypothesis, each $x_i = \phi_n(m_i)$ for $m_i < |V_n|$. Without loss of generality, suppose that $m_k > \cdots > m_1$. Thus, $\phi_{n+1}(2^{m_k} + \cdots + 2^{m_1}) = x$ since $2^{m_k} + \cdots + 2^{m_1}$ is the base 2 representation of a number less than $|V_{n+1}|$. Thus, ϕ_{n+1} is a bijection. We constructed it in such a way that it is in fact an isomorphism, and that ϕ_{n+1} extends ϕ_n follows from extensionality and the fact that the base 2 expansion of each number is unique. Therefore, $\phi : \omega \to HF$ defined by $\phi(n) = \phi_{n+1}(n)$ is an isomorphism. □

This defines HF inside ω. These arguments can be generalized to work for nonstandard models of PA and ZFCfin and can be formalized within PA and ZFCfin, thus proving their biinterpretability. These arguments have their origin in work of Ackermann [1]; see [19] for a historical discussion of their development. See [15, 16] for an extensive justification that ZFCfin, and thusly PA, formally satisfies our intuitive notion of finitary mathematics.

References

[1] W. Ackermann. *Die Widerspruchsfreiheit der allgemeinen Mengenlehre*, Math. Ann. **114** (1937), 305–315.

[2] W. Buchholz, S. Wainer. *Provably computable functions and the fast-growing hierarchy*, in **Contemporary Mathematics Volume 65: Logic and Combinatorics (Proceedings of a Summer Research Conference held August 4–10, 1985)**, American Mathematical Society, (1987), 179–198.

[3] G. Cantor. **Contributions to the founding of the theory of transfinite numbers. Translated, and provided with an introduction and notes, by Philip E. B. Jourdain**. Dover Publications, Inc., New York, N. Y., (1952).

[4] J. Dawson Jr. *What hath Gödel wrought?*, Synthese, **114 (1)** (Jan., 1998), 3–12.

[5] H. Enderton. *Elements of recursion Theory*, in **Handbook of Mathematical Logic**, edited by J. Barwise, North-Holland (1977) 527–566.

[6] H. Friedman. *Unprovable theorems in discrete mathematics*, lecture notes, (1999) http://www.math.ohio-state.edu/∼friedman

[7] G. Gentzen. *Die Widerspruchsfreiheit der reinen Zahlentheorie*, Math. Ann. **112 (1)** (1936), 493–565.

[8] G. Gentzen. *Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie*, Math. Ann. **119** (1943), 140-161.

[9] K. Gödel. *Über formal unentscheidbare Sätze der* Principia mathematica *und verwandter Systeme I* (1931), reprinted and translated as *On formally undecidable propositions of* Principia mathematica *and related systems I* in **Collected works. Vol. I. Publications 1929–1936.** S. Feferman, J. Dawson Jr., S. Kleene, G. Moore, R. Solovay, J. van Heijenoort, eds . The Clarendon Press, Oxford University Press, New York (1986), 144–195.

[10] R. L. Goodstein. *On the restricted ordinal theorem*, The Journal of Symbolic Logic **9 (2)** (Jun., 1944), 33–41.

[11] R. Kaye. **Models of Peano Arithmetic**, Oxford University Press (1991).

[12] J. Ketonen, R. Solovay. *Rapidly growing Ramsey functions*, The Annals of Mathematics, 2nd Ser., **113 (2)** (Mar., 1981), 267–314.

[13] L. A. S. Kirby, J. B. Paris. *Initial segments of models of Peano's axioms*. In **Set theory and hierarchy theory, V (Proc. Third Conf., Bierutowice, 1976)**, Lecture Notes in Math., Vol. 619, Springer, Berlin (1977), 211–226.

[14] G. Kreisel. *On the interpretation of nonfinitistic proofs: Part II*, The Journal of Symbolic Logic, **17 (1)** (Mar., 1952), 43–48.

[15] G. Kreisel. *Ordinal logics and the characterization of informal notions of proof*, **in Proceedings of the International Congress of Mathematicians. Edinburgh, 14–21 August 1958**, J.A. Todd, ed., Cambridge University Press (1960), 289–299.

[16] G. Kreisel. *Principles of proof and ordinals implicit in given concepts*, in **Intuitionism and proof theory**, A. Kino, J. Myhill, R. E. Veseley, eds., North-Holland (1970), 489–516.

[17] H. Levitz, *Transfinite ordinals and their notations: for the uninitiated*, http://www.cs.fsu.edu/∼levitz/research.html

[18] J. Paris, L. Harrington. *A mathematical incompleteness in Peano arithmetic*, in **Handbook of Mathematical Logic**, edited by J. Barwise, North-Holland (1977), 725–731.

[19] Ch. Parsons. *Developing Arithmetic in Set Theory without Infinity: some historical remarks*, History and Philosophy of Logic **8** (1987), 201–213.

[20] J. Rosenstein. **Linear orderings**, Pure and applied mathematics, no. 98. Academic Press, New York and London (1982).

[21] G. Sacks. **Higher recursion theory**, Perspectives in Mathematical Logic, Springer (1990).

[22] S. Simpson. *Unprovable theorems*, in **Contemporary Mathematics Volume 65: Logic and Combinatorics (Proceedings of a Summer Research Conference held August 4–10, 1985)**, American Mathematical Society (1987), 359–394.

[23] R. I. Soare. *The history and concept of computability.* In **Handbook of computability theory**, Stud. Logic Found. Math., 140, North-Holland, Amsterdam (1999), 3–36.

[24] J. Spencer. *Large numbers and unprovable theorems*, The American Mathematical Monthly, **90 (10)** (Dec., 1983), 669–675.

[25] J. von Neumann. *Zur Einführung der transfiniten Zahlen*, Acta Litterarum ac Scientiarum Regiae Universitatis Hungaricae Francisco-Josephinae, Sectio Scientiarum Mathematicarum **1** (1923), 199–208.

[26] S. Wainer. *A classification of the ordinal recursive functions.* Arch. Math. Logik Grundlagenforsch. **13** (1970), 136–153.