SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

An introduction to Goodstein's theorem

av

Anton Christenson

2019 - No K38

An introduction to Goodstein's theorem

Anton Christenson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Paul Vaderlind

2019

Abstract

Goodstein's theorem is a statement about the natural numbers, proved by Reuben Goodstein in 1944, and shown to be independent of Peano Arithmetic by Laurence Kirby and Jeff Paris in 1982. We give an introduction to the theorem, as well as a basic description of the two first-order theories (Peano Arithmetic and Zermelo Fraenkel set theory) relevant to our discussion of the theorem and its independence. We then develop the theory of well-ordered sets and ordinal numbers, leading in the end to a simple proof of Goodstein's theorem.

Contents

1 Introduction

We begin by introducing a new operation, which we will use to define a family of fastgrowing number sequences. After familiarizing ourselves with these sequences, we state the somewhat shocking Goodstein's theorem.

1.1 Complete base-n representations

It is a basic fact of arithmetic that for any base $n \geq 2$, every natural number has a unique base-n representation

$$\sum_{i=0}^{k} n^i c_i$$

where the coefficients c_i are natural numbers smaller than n. To make sure that this representation is completely unique, we follow these conventions:

- We write the terms in decreasing order.

$$2^2 + 2^5 + 2^6 \quad \to \quad 2^6 + 2^5 + 2^2$$

- We write coefficients to the right.[1]

$$3 \cdot 10^2 \quad \to \quad 10^2 \cdot 3$$

- We write n^k instead of $n^k \cdot 1$, n instead of n^1 and c instead of $n^0 \cdot c$. If a coefficient is 0, we leave out the term entirely.

$$5^3 \cdot 1 + 5^2 \cdot 0 + 5^1 \cdot 2 + 5^0 \cdot 4 \quad \to \quad 5^3 + 5 \cdot 2 + 4$$

The first two will be necessary later for an operation to be well-defined. The last one is mainly to keep our expressions neater.

Although the coefficients in a base-n representation are always smaller than n, the exponents may of course be larger. For instance:

$$100 = 2^6 + 2^5 + 2^2$$

If we also rewrite the exponents in base 2, we obtain a *complete* base-2 representation:

$$100 = 2^{2^2+2} + 2^{2^2+1} + 2^2$$

In general, we write a number m in complete base-n representation by first writing it in base n, then rewriting the exponents in base n, and continuing on in that manner until no numbers larger than n appears in the whole expression. We can describe this procedure recursively as follows:

[1] This is of course unusual, but we have our reasons, which will become clear later.

> To write a number in complete base-n, write out it's base-n representation, then write each exponent in complete base-n.

For another example, the complete base-3 representation of 1000 is obtained in two steps as follows:

$$1000 = 3^6 + 3^5 + 3^3 + 1 = 3^{3\cdot 2} + 3^{3+2} + 3^3 + 1$$

And here is a number where it takes three steps to obtain the complete base-2 representation:

$$8\,589\,934\,593 = 2^{33} + 1 = 2^{2^5+1} + 1 = 2^{2^{2^2+1}+1} + 1$$

Given a number m and two bases n and k, we define $(m)_{n\to k}$ to be the number obtained by starting with the complete base-n representation of m and then replacing every occurence of n with k. For instance:

$$(10)_{5\to 6} = (5\cdot 2)_{5\to 6} = 6\cdot 2 = 12$$
$$(10)_{3\to 4} = (3^2+1)_{3\to 4} = 4^2 + 1 = 17$$
$$(100)_{2\to 3} = (2^{2^2+2} + 2^{2^2+1} + 2^2)_{2\to 3} = 3^{3^3+3} + 3^{3^3+1} + 3^3 = 228\,767\,924\,549\,637$$

1.2 Goodstein sequences

Definition 1. The Goodstein sequence $G_n(m)$ is defined recursively by

$$G_2 := m$$
$$G_{n+1} := (G_n)_{n\to n+1} - 1$$

If it eventually happens that $G_k = 0$, we say that the sequence terminates at base k.

In words, this procedure amounts to repeatedly increasing the base and decreasing the number. For instance, starting with $G_2(4) = 4 = 2^2$ we get

$$G_3(4) = (2^2)_{2\to 3} - 1 = 3^3 - 1 = 3^2\cdot 2 + 3\cdot 2 + 2$$

and then

$$G_4(4) = (3^2\cdot 2 + 3\cdot 2 + 2)_{3\to 4} - 1 = 4^2\cdot 2 + 4\cdot 2 + 1$$

and so on. The table below shows the complete base-n representations of $G_n(4)$ and $G_n(100)$ for $n \le 10$:

n	$G_n(4)$	$G_n(100)$
2	2^2	$2^{2^2+2} + 2^{2^2+1} + 2^2$
3	$3^2 \cdot 2 + 3 \cdot 2 + 2$	$3^{3^3+3} + 3^{3^3+1} + 3^2 \cdot 2 + 3 \cdot 2 + 2$
4	$4^2 \cdot 2 + 4 \cdot 2 + 1$	$4^{4^4+4} + 4^{4^4+1} + 4^2 \cdot 2 + 4 \cdot 2 + 1$
5	$5^2 \cdot 2 + 5 \cdot 2$	$5^{5^5+5} + 5^{5^5+1} + 5^2 \cdot 2 + 5 \cdot 2$
6	$6^2 \cdot 2 + 6 + 5$	$6^{6^6+6} + 6^{6^6+1} + 6^2 \cdot 2 + 6 + 5$
7	$7^2 \cdot 2 + 7 + 4$	$7^{7^7+7} + 7^{7^7+1} + 7^2 \cdot 2 + 7 + 4$
8	$8^2 \cdot 2 + 8 + 3$	$8^{8^8+8} + 8^{8^8+1} + 8^2 \cdot 2 + 8 + 3$
9	$9^2 \cdot 2 + 9 + 2$	$9^{9^9+9} + 9^{9^9+1} + 9^2 \cdot 2 + 9 + 2$
10	$10^2 \cdot 2 + 10 + 1$	$10^{10^{10}+10} + 10^{10^{10}+1} + 2 \cdot 10^2 + 10 + 1$

We see that $G_n(4)$ grows steadily, but not very quickly: $G_{10}(4) = 211$ is still easily expressed in ordinary decimal notation. $G_n(100)$ grows much faster, and a simple analysis shows that

$$G_{10^{10}}(100) > 10^{10^{10^{10}}}$$

so it shows no signs of slowing down any time soon.

At the other extreme, the sequences $G_n(0)$, $G_n(1)$, $G_n(2)$ and $G_n(3)$ terminate almost immediately, at bases 2, 3, 5 and 7 respectively. But every later sequence looks to be diverging, each more quickly than the previous one:

0

1, 0

2, 2, 1, 0

3, 3, 3, 2, 1, 0

4, 26, 41, 60, 83, 109, 139, 173, 211, 253, 299, 348, 401, 458, 519 ...

5, 27, 255, 467, 775, 1197, 1751, 2454, 3325, 4382, 5643, 7126, 8849 ...

6, 29, 257, 3125, 46655, 98039, 187243, 332147, 555551, 885775, 1357259 ...

The natural question at this point is: does $G_n(4)$ terminate? Looking at the first hundred million terms or so, it looks like it does not. But surprisingly it *does* terminate; it just takes so long to do so that a direct computation will never reach that point. In section 5.2 we will see that that the final base for $G_n(4)$ is:

$$n = 3 \cdot 2^{402\,653\,211} - 1$$

One might then reasonably ask: what is the smallest m such that $G_n(m)$ does not terminate? The shocking answer is that $G_n(m)$ *always* terminates, regardless of how big m is. This is *Goodstein's theorem*.

2 Prerequisites and historical context

The next two sections describe the two different first-order theories that are relevant to our discussion of Goodstein's theorem. For a short introduction to the language of first-order logic, see appendix A.

2.1 Peano Arithmetic

The natural numbers

$$0, 1, 2, 3, 4, 5 \ldots$$

and their arithmetic

$$1 + 2 = 3 \qquad 2 \cdot 3 = 6$$

is one of the first mathematical theories that is taught to children. Peano arithmetic (PA) attempts to formalize this theory into first order logic, using the following primitive notions:

- A nullary function 0 (zero)
- A unary function S (successor)
- A binary function $+$ (addition)
- A binary function $\cdot$ (multiplication)

We of course have an intuitive notion of how these "should" behave, so the question becomes: what is the "simplest" possible set of axioms, that still allows us to do the things we want with the natural numbers?

We can describe the "shape" of the set of natural numbers, in terms of how the successor function S acts on it:

1. $S(a) \neq 0$
2. $S(a) = S(b) \to a = b$
3. $\varphi(0) \wedge \forall a\,[\varphi(a) \to \varphi(S(a))] \to \forall b\,[\varphi(b)]$

And we also assert the basic properties of addition and multiplication as axioms:

7. $a + 0 = a$
8. $a + S(b) = S(a + b)$
9. $a \cdot 0 = 0$
10. $a \cdot S(b) = a \cdot b + a$

Extensions

Working in first order logic, the properties of addition and multiplication must be included as axioms. Since it seems quite natural to be able to *define* operations recursively as above, we may take this as a sign that the first order setting is not good enough for us. Suppose for example that after a while of playing around with addition and multiplication, we decide that we also want to define exponentiation. Do we need *another* pair of axioms for this? Fortunately not.

Using only the primitives that we've already got, and some ingenuity, it is possible to construct a formula $\varphi(a, b, c)$ which is equivalent to $a^b = c$. Then we can introduce exponentiation as an extension by definition, and *prove* that the identities

$$a^0 = 1$$
$$a^{S(b)} = a^b \cdot a$$

hold. Thus it is not necessary to include these as axioms in PA.

In fact, one can show that any function $f : \mathbb{N}^k \to \mathbb{N}$ that is *computable* (by a Turing machine, for instance, although there are many alternative formalizations that give the same class of functions) can be introduced into PA in the same way. Thus it is possible to define the basebumping operation $(m)_{n\to k}$ and then the Goodstein sequence $G_n(m)$ within PA. The technical details of how to do so does not matter for our purposes, we just want to know that it is possible to state Goodstein's theorem in PA.

Removing multiplication

We might try to also leave out the axioms for multiplication and define it in terms of addition, but this does not work. The theory we end up with when we remove multiplication is called Presburger arithmetic, and it is known to be much weaker than Peano arithmetic: it can be proved to be consistent, complete and decidable. This means that for any sentence P, either P or $\neg P$ (but never both) can be deduced from the axioms, and it is possible for an algorithm to decide which of them is. So in some sense it is "too simple to be interesting". This is in contrast to Peano arithmetic, which is undecidable: there are statements (such as Goodstein's theorem) that cannot be proven true or false.

2.2 Zermelo-Fraenkel set theory

Zermelo Fraenkel set theory (ZF) formalizes the class of *hereditary well-founded sets*, using only the binary membership predicate $\in$, with the following axioms:

Extensionality

$$(x \in A \leftrightarrow x \in B) \to A = B$$

If two sets have the same elements, they are equal. An alternative approach is to *define* two sets as being equal if they have the same elements, in which case

one instead needs the substitution axiom $a = b \in X \to a \in X$. In either case the intuition behind the axiom is that sets are completely determined by their elements.

Union

$$\forall X\, \exists Y\, [\, y \in Y \leftrightarrow \exists x \in X\, (y \in x)\,]$$

If X is a set, then there is a set Y containing all the elements of all the elements of X. We denote this set by $\bigcup X$ and introduce the shorthand $a \cup b$ for $\bigcup\{a, b\}$.

Power set

$$\forall X\, \exists Y\, [\, y \in Y \leftrightarrow \forall x \in y\, (x \in X)]$$

If X is a set, then there is a set Y containing all the subsets of X. We denote this set by $\mathcal{P}(X)$.

Replacement

$$\forall X\, \exists Y\, [\, y \in Y \leftrightarrow \exists x \in X\, (\varphi(x, y))\,]$$

where φ is any binary predicate satisfying $\varphi(x, y_1) \wedge \varphi(x, y_2) \to y_1 = y_2$. Intuitively, φ behaves like a partial class function F, and Y is the image of X under this function.

Infinity

$$\exists X \neq \varnothing\ \ \forall a \in X\ \ \exists b \in X\ \ a \in b$$

There is a set containing every element of an infinite ascending chain

$$x_0 \in x_1 \in x_2 \in x_3 \ldots .$$

Foundation

$$\forall X \neq \varnothing\ \ \exists a \in X\ \ \forall b \in X\ \ b \notin a$$

The $\in$ relation is well-founded: every non-empty set has a $\in$-minimal element. This implies that there are no infinite descending chains

$$x_0 \ni x_1 \ni x_2 \ni x_3 \ldots$$

Assuming the axiom of dependent choice, the converse implication also holds.

See appendix B.1 for how to construct some other basic sets (the existence of which is often taken as axioms) using only the axioms above.

Classes

Although everything in ZF is a set, it is useful to introduce the informal notion of a *class*, which is any collection of sets. If t is a term and φ is a formula, then $\{ t \mid \varphi \}$ denotes the class of all sets t such that φ is true. All sets are classes, but not all classes are sets.

Example 1. Consider the class $V := \{ x \mid x \notin x \}$. By definition, for all sets x

$$x \in V \leftrightarrow x \notin x$$

so if V itself were a set, we would have

$$V \in V \leftrightarrow V \notin V$$

which is a contradiction.

A class that is not a set is called a *proper* class. Intuitively, proper classes are "too big" to be sets. The proper class V actually contains *every set* (for any set x, the axiom of foundation applied to the set $\{x\}$ shows that $x \notin x$), so it is the largest possible class.

2.3 Natural numbers as sets

We now describe a standard way to construct the natural numbers as sets within ZF, due to von Neumann. First we pick a set to represent the number 0, and the empty set seems a natural choice:

$$0 := \varnothing$$

Next we define the successor function S. Given a set x (which represents some natural number), we define its successor as follows:

$$S(x) := x \cup \{x\}$$

Starting with $0 := \varnothing$ and applying $S(x) := x \cup \{x\}$ repeatedly we get a sequence of sets representing the natural numbers;

$$\begin{aligned}
1 &:= S(0) = \{\varnothing\} = \{0\} \\
2 &:= S(1) = \{\varnothing, \{\varnothing\}\} = \{0, 1\} \\
3 &:= S(2) = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\} \\
4 &:= S(3) = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\} = \{0, 1, 2, 3\}
\end{aligned}$$

and so on. One can then prove (see appendix B.2) that there is a set containing all natural numbers

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

and that (definining addition and multiplication by recursion) this is a model of PA.

There are alternative definitions that also give valid models of PA. For example, Ernst Zermelo (the Z in ZF) suggested $S(x) := \{x\}$. The reason for using von Neumann's slightly more complicated successor function is that it gives the natural numbers some extra nice properties:

1. The cardinality of each natural number is itself. For example

$$3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$$

   is a set with 3 elements.

2. Each natural number consists precisely of the natural numbers that precedes it. For example $3 = \{0, 1, 2\}$. Thus we can define the order relation $<$ on the natural numbers to be precisely the membership relation $\in$ (we say that $m < n$ if and only if $m \in n$).

This is aesthetically pleasing, but might not seem to give us anything new if we are already familiar with the natural numbers. However, when we later extend von Neumann's construction beyond the natural numbers, these properties will become more important.

2.4 Is ZF more powerful than PA?

PA describes the natural numbers, and one can do quite alot with this theory (for instance, define any computable function, and prove various theorems about arithmetic), but it seems impossible to do all of mathematics inside of it. Even relatively basic concepts such as the real numbers seem impossible to define in PA.

In the theory of ZF, everything is a set, but we can construct all sorts of things as certain sets. We saw in the last section how to construct a model of PA inside of ZF, but that is only the beginning: real and complex numbers, functions and relations between sets, and much more, can all be constructed as sets. Thus ZF can be used as a common foundation for most "ordinary" mathematics.

Based on this, it seems natural to claim that ZF is more powerful than PA in some sense. But how can we formalize and prove such a statement? After all, if we can talk about real numbers within ZF (which only "knows" about sets), might it not be possible to also talk about real numbers within PA (which only "knows" about natural numbers)? Maybe it is even possible to construct a model of ZF within PA?

One way to prove that this is not possible is to exhibit a statement which can be stated within PA, but that can only be proven true within ZF: this is where Goodstein's theorem comes in! It can be proven true in ZF but not in PA, and thus shows that ZF is indeed more powerful than PA.

2.5 History

Reuben Goodstein introduced what we now call Goodstein sequences in a 1944 paper *On the restricted ordinal theorem* [2]. In 1982, Laurie Kirby and Jeff Paris published a proof [5] that Goodstein's theorem is not provable within PA. This was not the first such independence result, but Kirby and Paris wrote that it was

> "perhaps the first which is, in an informal sense, purely number-theoretic in character (as opposed to metamathematical or combinatorial)"

and for this reason it is a quite famous result. While Gödel's first incompleteness theorem (published in 1931) showed that there are true statements about the natural numbers that cannot be proven from within PA, Goodstein's theorem is the first one that actually *seems* like a statement about the natural numbers.

Unfortunately, the details of the independence proof are quite technical and thus beyond the scope of this text, so we will not say too much more about it. Instead we will focus on developing the theory necessary to prove Goodstein's theorem within ZF.

3 Well-ordered sets

This section will develop some of the theory of well-ordered sets, preparing us to tackle ordinal numbers in the next section.

3.1 Definition and examples

Definition 2. Let X be a set equipped with a binary relation $<$. We say that X is *linearly ordered* by $<$ if

1. For all $a, b \in X$, exactly one of $a < b$, $a = b$ and $a > b$ holds. (trichotomy)
2. For all $a, b, c \in X$, if $a < b < c$, then $a < c$. (transitivity)

and that X is *well-ordered* by $<$ if it additionally holds that

3. Every non-empty subset of X has a minimal element. (well-foundedness)

Remark 1. Of course, any ordered set is really a pair $(X, <)$, since a single set can be equipped with different orders, but the relevant order is almost always clear from the context.

Remark 2. Linear orders are also known as *total orders*, which emphasises the fact that they are partial orders where all elements are comparable. The term linear order instead hints at the visual intuition of picturing the elements of a linearly ordered set as being laid out on a line such that $a < b$ if a is placed somewhere to the left of b.

Remark 3. More explicitly, the well-foundedness property says that if S is a non-empty subset of X, then

$$\exists a \in S \ \ \forall b \in S \ \ b \not< a.$$

Compare this to the axiom of foundation, which states that if X is any non-empty set, then

$$\exists a \in X \ \ \forall b \in X \ \ b \notin a.$$

Thus, the axiom of foundation is so named because it essentially says that the membership relation is well-founded on the class of all sets.

Example 2. In the von Neumann construction we are using, each natural number n is the set

$$\mathbf{n} = \{0, 1, 2, \ldots n-1\}$$

which is well-ordered by $<$. We write the natural number in bold to emphasize that we are thinking of it as a well-ordered set.

Example 3. The simplest example of an infinite well-ordered set is the set of all natural numbers $\mathbb{N}$. A simple example of a set that is linearly ordered but not well-ordered is $\mathbb{Z}$.

Example 4. If T is a well-ordered set, and S is any subset of T, we can make S into a well-ordered set by letting it inherit the order relation from T. In other words, for any $a, b \in S$ we define $a <_S b$ if and only if $a <_T b$. The trichotomy, transitivity and well-foundedness of $<_S$ follow directly from the corresponding properties of $<_T$.

The following lemma follows directly from the definition, but is very important.

Lemma 1. *A well-ordered set contains no infinite descending chain*

$$x_0 > x_1 > x_2 > \ldots$$

Proof. If such a chain existed, the elements of the chain would form a non-empty subset with no least element. □

Example 5. The set of non-negative rational numbers $\mathbb{Q}^{\geq 0}$ has a smallest element 0, but there is an infinite descending chain

$$\frac{1}{1} > \frac{1}{2} > \frac{1}{3} > \frac{1}{4} \ldots$$

so it is not well-ordered by $<$.

It is essentially the no-descending-chains-property that allows us to make recursive definitions and inductive proofs on the natural numbers. The fact that this property holds for all well-ordered sets will allow us to generalize these to *transfinite* recursion and induction.

3.2 Order isomorphism and initial segments

Definition 3. Suppose that X is well-ordered by $<_X$ and Y is well-ordered by $<_Y$. We say that X and Y are *(order) isomorphic* if there is a bijective function $f : X \to Y$ such that $a <_X b$ if and only if $f(a) <_Y f(b)$. We write this as $X \cong Y$, or $X \cong_f Y$ if we wish to specify the isomorphism. Order isomorphism is

- Reflexive: $A \cong_{\mathrm{id}} A$
- Symmetric: $A \cong_f B \to B \cong_{f^{-1}} A$
- Transitive: $A \cong_f B \cong_g C \to A \cong_{g \circ f} C$

so it is an equivalence relation on the class of well-ordered sets. We essentially consider isomorphic well-ordered sets as "the same" well-ordered set.

Definition 4. If W is a well-ordered set and x is any element of W, then

$$W_{<x} := \{w \in W \mid w < x\}$$

is an *inital segment* of W. By letting it inherit the order relation from W (see example 4), it is also a well-ordered set.

Example 6. Every natural number is an inital segment of $\mathbb{N}$:

$$\forall n \in \mathbb{N}\, (\mathbb{N}_{<n} = \mathbf{n})$$

Lemma 2. *No well-ordered set is isomorphic to an initial segment of itself.*

Proof. If $W \cong_f W_{<x}$, then

$$x,\ f(x),\ f(f(x)),\ f(f(f(x))),\ \ldots$$

is an infinite decreasing chain in W. □

3.3 Arithmetic

Let's now do some arithmetic on well-ordered sets. Given two well-ordered sets X and Y, we are going to construct new well-ordered sets

$$X + Y \qquad X \cdot Y \qquad X^Y$$

We of course want to do this such that the operations are invariant under isomorphism: if $X \cong X'$ and $Y \cong Y'$, then $X + Y \cong X' + Y'$ and similarly for the other operations. This happens by itself if we make sure that our definitions only depend on the the way the elements of X and Y are ordered, rather than what the elements actually are.

Addition

An intuitive way of adding X and Y is to place all the elements of X "before" or "to the left of" all the elements of Y. When making the formal definition, we need to make sure to keep the elements of X and Y separate, since we want the definition to be independent of whether X and Y share any elements. We can do this by "tagging" them with 0 and 1 respectively:

$$X \times \{0\} = \{\, (x, 0) \mid x \in X \,\}$$

$$Y \times \{1\} = \{\, (y, 1) \mid y \in Y \,\}$$

Then it does not matter if some element a of X also happens to be an element of Y, since $(a, 0) \in X \times \{0\}$ and $(a, 1) \in Y \times \{1\}$ are still distinct. Thus we define:

$$X + Y := (X \times \{0\}) \cup (Y \times \{1\})$$

Definition 5. For any two well-ordered sets $(X, <_X)$ and $(Y, <_Y)$, we define $X + Y$ to be the set

$$(X \times \{0\}) \cup (Y \times \{1\})$$

equipped with the following relation:

- $(x, 0) < (x', 0)$ if $x <_X x'$ (for all x, $x' \in X$)
- $(x, 0) < (y, 1)$ (for all $x \in X$, $y \in Y$)
- $(y, 1) < (y', 1)$ if $y <_Y y'$ (for all y, $y' \in Y$)

In other words, to order two elements, we first try to compare them by their last coordinates. If they are equal, we move on to comparing the first coordinates.[2] This relation is...

Trichotomous: By definition.

Transitive: Suppose that $(a_1, b_1) < (a_2, b_2) < (a_3, b_3)$. We cannot have $b_1 > b_3$, since that would imply either $b_1 > b_2$ or $b_2 > b_3$.

- If $b_1 < b_3$ then $(a_1, b_1) < (a_3, b_3)$ by definition.
- If $b_1 = b_3 = 0$, then $a_1 <_X a_2 <_X a_3$ which implies $a_1 <_X a_3$ and then $(a_1, b_1) < (a_3, b_3)$.
- If $b_1 = b_3 = 1$, then $a_1 <_Y a_2 <_Y a_3$ which implies $a_1 <_Y a_3$ and then $(a_1, b_1) < (a_3, b_3)$.

[2] With the small asterisk that we technically need to look at the value of the second coordinates to know if we should compare the first coordinates by $<_X$ or by $<_Y$.

Well-founded: Let S be a non-empty subset of $X+Y$. If $\{\, x \in X \mid (x,0) \in S \,\}$ is non-empty, then it has a $<_X$-minimal element x_m, and $(x_m, 0)$ is the minimal element of S. Otherwise $\{\, y \in Y \mid (y,1) \in S \,\}$ is non-empty and has a $<_Y$-minimal element y_m, in which case $(y_m, 1)$ is the minimal element of S.

...so $X+Y$ is indeed a well-ordered set. Adding finite well-ordered sets works similarly to adding natural numbers:

$$\mathbf{2} + \mathbf{3} = \mathbf{2} \times \{0\} \cup \mathbf{3} \times \{1\} = \{(0,0), (1,0), (0,1), (1,1), (2,1)\} \cong \{0,1,2,3,4\} = \mathbf{5}$$

Addition involving infinite well-ordered sets can be more counterintuitive. Let's compare what happens when we add $\mathbf{1} = \{0\}$ to the left and right of $\mathbb{N}$:

$$\mathbf{1} + \mathbb{N} = \mathbf{1} \times \{0\} \cup \mathbb{N} \times \{1\} = \{(0,0)\} \cup \{(1,0), (1,1), (1,2), (1,3) \ldots\}$$

which is isomorphic to $\mathbb{N}$ under $(a,b) \mapsto a+b$.

$$\mathbb{N} + \mathbf{1} = \mathbb{N} \times \{0\} \cup \mathbf{1} \times \{1\} = \{(0,0), (1,0), (2,0), (3,0) \ldots\} \cup \{(0,1)\}$$

which is *not* isomorphic to $\mathbb{N}$ since it has a greatest element. Thus addition of well-ordered sets is not commutative.

Multiplication

The visual intuition is slightly more complicated for the multiplication: we will think of the product of X and Y as Y copies of X. More precisely, start by picturing the elements of Y as points along a line, then replace each such point with a separate copy of X. This idea is realized by the following ordering:

Definition 6. For any two well-ordered sets X and Y, we define $X \cdot Y$ to be the set $X \times Y = \{\, (x,y) \mid x \in X \wedge y \in Y \,\}$ equipped with the relation:

- $(x,y) < (x',y')$ if $y <_Y y'$
- $(x,y) < (x',y)$ if $x <_X x'$

Remark 4. Once again, this ordering can be described by "try to compare the last coordinates first, and if they are equal, move on to the first coordinates". This is similar to the *lexicographical ordering* used to order the words in a dictionary: to decide which of two words comes first, the first letters of the two words are compared. If they are equal, the second letters are compared, and so on. In the setting of well-ordered sets, the convention is instead to use *reverse* lexicographical order: start by comparing the last coordinate, then move on to the first if needed.

This relation is...

Trichotomous: By definition.

Transitive: Suppose that $(x_1, y_1) < (x_2, y_2) < (x_3, y_3)$. Then either $y_1 < y_3$ and we are done, or $y_1 = y_2 = y_3$, in which case $x_1 < x_2 < x_3$ and we are done.

Well-founded: Any non-empty subset S of $X \cdot Y$ has a minimal element (x_m, y_m) where y_m is the $<_Y$-minimal element of

$$\{\, y \in Y \mid \{\, x \in X \mid (x, y) \in S \,\} \neq \varnothing \,\}$$

and x_m is the $<_X$-minimal element of $\{\, x \in X \mid (x, y_m) \in S \,\}$.

...so $X \cdot Y$ is indeed a well-ordered set. Just like with addition, multiplication of finite sets is familiar...

$$\mathbf{2} \cdot \mathbf{3} = \{(0,0), (1,0), (0,1), (1,1), (0,2), (1,2)\} \cong \mathbf{6}$$

...but multiplying infinite sets can be more counter-intuitive:

Example 7. What does $\mathbb{N} \cdot \mathbf{2}$ look like? As a set, it consists of all ordered pairs (n, b) with $n \in \mathbb{N}$ and $b \in \{0, 1\}$. To determine which of two elements (n_1, b_1) and (n_2, b_2) is larger, we first try to compare b_1 and b_2. If $b_1 = b_2$, we compare n_1 and n_2 instead. Thus we get the following ordering:

$$(0,0) < (1,0) < (2,0) < \cdots < (0,1) < (1,1) < (2,1) \cdots$$

This is isomorphic to $\mathbb{N} + \mathbb{N}$; in fact, $\mathbb{N} \cdot \mathbf{2}$ and $\mathbb{N} + \mathbb{N}$ are identical as sets.

Let us next look at $\mathbf{2} \cdot \mathbb{N}$. As a set, its elements are all ordered pairs (b, n) with $b \in \{0, 1\}$ and $n \in \mathbb{N}$. So far this looks very similar to before, but this time when we are comparing (b_1, n_1) and (b_2, n_2) we compare n_1 and n_2 before b_1 and b_2. This leads to the following ordering:

$$(0,0) < (1,0) < (0,1) < (1,1) < (0,2) < (1,2) \cdots$$

which is isomorphic to $\mathbb{N}$ under $(b, n) \mapsto b + 2n$.

So far we found that $\mathbb{N} \cdot \mathbf{2} \cong \mathbb{N} + \mathbb{N}$ and that $\mathbf{2} \times \mathbb{N} \cong \mathbb{N}$. Might it be the case that $\mathbb{N} + \mathbb{N} \cong \mathbb{N}$? No, because $\mathbb{N}$ is isomorphic to an inital segment of $\mathbb{N} + \mathbb{N}$, and we know from lemma 2 that a well-ordered set cannot be isomorphic to an inital segment of itself.

Thus we have that

$$\mathbb{N} \cdot \mathbf{2} \cong \mathbb{N} + \mathbb{N} \ncong \mathbb{N} \cong \mathbf{2} \cdot \mathbb{N}$$

which shows that multiplication of well-ordered sets is not commutative.

Exponentiation

Next we want to define exponentiation of well-ordered sets. It is difficult to provide a visual intution for this operation, so we instead try to generalize our understanding of exponentiation as repeated multiplication: it seems reasonable

to expect that $X^{\mathbf{n}}$ should be isomorphic to $X \cdot (X \cdot (X \cdot (\ldots \cdot X)))$. As a set, this is esentially the set of n-tuples $(x_0, x_1, x_2, \ldots, x_{n-1})$ where $x_i \in X$. Thus we guess that $X^{\mathbb{N}}$ should be the set of infinite sequences

$$x_0, x_1, x_2, \ldots$$

where $x_i \in X$. For example, $\mathbf{2}^{\mathbb{N}}$ would consist of infinite sequences of 1's and 0's. But how should we compare two different sequences? It seems natural to start looking from the beginning until we find a point where they differ (this is for instance how we compare the decimal (or binary) expansions of two numbers). More precisely, we say that $a_i < b_i$ if

$$\exists n \, (a_n < b_n \wedge \forall m < n \, (a_m = b_m))$$

But then there is an infinite decreasing chain of sequences:

$$\begin{aligned}
&1, 0, 0, 0, 0, 0, 0, 0, \ldots \\
&0, 1, 0, 0, 0, 0, 0, 0, \ldots \\
&0, 0, 1, 0, 0, 0, 0, 0, \ldots \\
&0, 0, 0, 1, 0, 0, 0, 0, \ldots \\
&\vdots
\end{aligned}$$

so this is not a well-ordering. What if we start comparing from the end instead? We say that $a_i < b_i$ if

$$\exists n \, (a_n < b_n \wedge \forall m > n \, (a_m = b_m))$$

This solves the previous problem, but creates a new issue. Now the following two sequences are incomparable:

$$\begin{aligned}
&1, 0, 1, 0, 1, 0, 1, 0, \ldots \\
&0, 1, 0, 1, 0, 1, 0, 1, \ldots
\end{aligned}$$

The way to avoid both these issues is to start comparing from the end, but require the individual sequences to be finite, in the sense that all but a finite number of entries in the sequence are zero. We generalize this idea as follows:

Definition 7. A function between well-ordered sets $f : Y \to X$ is said to have *finite support* if all but a finite number of elements of Y map to the least element of X.

Definition 8. If X and Y are well-ordered sets, we let X^Y be the set of functions from Y to X with finite support. We equip this set with the following ordering: for any two functions $f, g : Y \to X$, we say that $f < g$ if

$$\exists y \in Y \, (f(y) < g(y) \wedge \forall y' > y \, (f(y') = g(y')))$$

This is an infinite analogue to the reverse lexicographical ordering.

This relation is...

Trichotomous: Let f and g be arbitrary functions from Y to X with finite support. The set of all $y \in Y$ such that $f(y) \neq g(y)$ is finite. If it is empty, then $f = g$. Otherwise, it contains a greatest element y'. If $f(y') < g(y')$, then $f < g$, and vice versa.

Transitive: Suppose that $f < g < h$, and denote the greatest element where f and g differ by y_1, and the greatest element where g and h differ by y_2. If $y_1 = y_2$, then $f(y_1) < g(y_1) < h(y_1)$, and it is clear that $f < h$. If $y_1 < y_2$, then $f(y_2) = g(y_2) < h(y_2)$. And if $y_1 > y_2$, then $f(y_1) < g(y_1) = h(y_1)$.

Well-founded: Let $\{f_i\}$ be a non-empty set of functions from Y to X. We are going to gradually reduce the size of this set by removing non-minimal elements, until it contains only one element, which will be the minimal element of the original set. For every f_i, denote by y_i the greatest element such that $f_i(y_i) \neq 0$. Then $\{y_i\}$ is a non-empty subset of Y, so it has a least element y_0. Discard all f_i such that $y_i \neq y_0$. Then look at the value of the remaining f_i on y_0. Discard all f_i that have a non-minimal value. Now the remaining f_i agree on all the values greater than or equal to y_0. Thus we can equivalently consider them as functions from the segment of Y that is smaller than y_0. Repeat the same procedure from the beginning, to obtain $y_1 < y_0$. Repeat until $y_k = y_{\min}$, the smallest element of Y. The remaining f_i agree on all values, which means that only one function $f_{\min}$ remains, which by construction is less than or equal to each element of $\{f_i\}$.

...so X^Y is indeed a well-ordered set.

4 Ordinal numbers

The natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ have mainly two applications in day to day life: measuring the size (cardinality) of sets, and ordering sets. In language we distinguish between these two cases: "three" is a *cardinal* number, while "third" is an *ordinal* number, but we usually think of the number 3 as being the same mathematical object in both cases. We can get away with using the same set $\mathbb{N}$ for both these purposes as long as we are talking about finite sets, but when we start measuring and ordering *infinite* sets, cardinals and ordinals are no longer the same. We saw in the previous chapter that the sets $\mathbb{N}$ and $\mathbb{N} + \mathbb{N}$ are not isomorphic as ordered sets, despite having the same cardinality (that is; we can find a bijection between the sets, but we cannot make that bijection order-preserving).

The ordinal analogue to cardinality is that of "order type". The ordinal numbers are constructed such that each well-ordered set X is isomorphic to exactly one ordinal number $\mathrm{ord}(X)$, the order type of X. Since every ordinal

is itself a well-ordered set of its own order type, another way of thinking about ordinals is as canonical representatives for the equivalence classes of well-ordered sets under isomorphism. This is analogous to how each natural number is a canonical representative for the class of finite sets of the same size.

4.1 Counting beyond infinity

In an informal sense the ordinals will allow us to continue counting "beyond infinity". Before doing things rigorously, let's just keep on counting for a while, making up new names for things as we go along.

The natural numbers are built upon these two rules:

1. 0 is a natural number.
2. If n is a natural number, then $n + 1$ is a bigger natural number.

which (with an appropriate naming scheme) gives an infinite sequence

$$0 \quad 1 \quad 2 \quad 3 \quad \dots$$

which we are very familiar with. The ordinals add a third rule, which allows us to always find a number "after" the "...".

1. 0 is an ordinal number
2. If α is an ordinal number, then $\alpha + 1$ is a bigger ordinal number.
3. If α_i is a sequence of ordinal numbers, there is some number β such that $\alpha_i < \beta$ for all α_i.

For instance, there is some ordinal, let's call it ω, that is greater than all the natural numbers:

$$0 \quad 1 \quad 2 \quad 3 \quad \dots \quad \omega$$

This is an infinite number, but we can still apply the first rule to get an even bigger number, $\omega + 1$. Continuing in this way, we get a *new* infinite sequence, and we make up a new name for the number at the end of this sequence:

$$\omega + 1 \quad \omega + 2 \quad \omega + 3 \quad \dots \quad \omega + \omega = \omega \cdot 2$$

And then we can repeat:

$$\omega \cdot 2 + 1 \quad \omega \cdot 2 + 2 \quad \omega \cdot 2 + 3 \quad \dots \quad \omega \cdot 3$$

We recognize that just repeating this step over and over again will never get us further than numbers of the form $\omega \cdot k$ for some natural number k. Is that as large as the ordinal numbers get? Of course not! We simply apply rule 3 to get an ordinal bigger than all ordinals of the form $\omega \cdot k$:

$$\omega \cdot 1 \quad \omega \cdot 2 \quad \omega \cdot 3 \quad \dots \quad \omega \cdot \omega = \omega^2$$

We can use the same idea to move beyond numbers of the form ω^k:

$$\omega^1 \quad \omega^2 \quad \omega^3 \quad \dots \quad \omega^\omega$$

But what should we name the number that comes at the end of this sequence?

$$\omega \quad \omega^\omega \quad \omega^{\omega^\omega} \quad \dots \quad \omega^{\omega^{\omega^{\cdot^{\cdot}}}} = \varepsilon_0$$

Here we have reached the point where combining a finite number of ω:s with addition, multiplication and exponentiation no longer suffices, and we have to make up a new name (or introduce some new notation such as ${}^\omega\omega$ or $\omega \uparrow\uparrow \omega$).

We cannot name all the ordinals, since there are uncountably many of them. This is not new; we know that we cannot name "most" real numbers for the same reason. But here the situation is even worse; there is no general naming scheme which would allow us to name arbitrarily large ordinals. For any naming scheme, there is a point beyond which the scheme cannot describe *any* ordinal. The good news is that for our purposes we will only need the ordinals smaller than ε_0, so we will not have to worry about this.

4.2 Ordinals as sets

Let's now go back to the beginning and construct the ordinals more rigorously. The idea (which is due to von Neumann) is to construct each ordinal as the well-ordered set of all smaller ordinals. We have already done this for the finite ordinals (formerly known as "the natural numbers"):

$$0 = \{\}, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\} \dots$$

By collecting them all together in a set we get the smallest infinite ordinal:

$$\omega = \{0, 1, 2, 3, \dots\}$$

The next ordinal after that is

$$\{0, 1, 2, 3, \dots \omega\}$$

which is isomorphic to $\mathbb{N} + \mathbf{1}$. We can continue making larger ordinals this way, but rather than trying to define a ordinal as a number that can be reached after some number of steps in this process, we describe directly what an ordinal looks like as a set.

Definition 9. A class T is called transitive if $a \in b \in T \implies a \in T$. Equivalently:

$$x \in T \to x \subseteq T$$
$$\bigcup T \subseteq T$$

Example 8. The class V of all sets is transitive, since every element of a set is a set.

Definition 10. An *ordinal* is a transitive set of transitive sets. We denote the class of all ordinals by Ω.

Lemma 3. *The class Ω is transitive: every element of an ordinal is an ordinal.*

Proof. Suppose that $x \in \alpha \in \Omega$. Then x is transitive, since it is an element of α. Furthermore, every element of x is also an element of α (since α is transitive) and thus transitive. It follows that $x \in \Omega$. □

Thus, a set is an ordinal if and only if it is a transitive set of ordinals, and a subset of an ordinal is an ordinal if and only if it is transitive.

Lemma 4. *The ordinals form a proper class; there is no "set of all ordinals".*

Proof. We have established that Ω is a transitive class of transitive sets. If it were also a set, it would be an ordinal, and then we would have $\Omega \in \Omega$, contradicting the axiom of foundation. □

Any ordinal γ can be considered as an ordered set $(\gamma, \in)$.
The relation $\in$ is ...

Trichotomous: For any sets x and y, it follows from the axiom of foundation that *at most one* of these statements can be true:

$$x \in y \qquad x = y \qquad x \ni y$$

If at least one of them are true, we say that x and y are comparable. Otherwise, we write $x \parallel y$ and say that x and y are incomparable.
Now suppose that the set

$$\{\, x \in \gamma \mid \exists y \in \gamma\, (x \parallel y) \,\}$$

is non-empty. Let β_x be the $\in$-minimal element of this set, and let β_y be the $\in$-minimal element of the set $\{\, y \in \gamma \mid \beta_x \parallel y \,\}$.
Notice that any element α of β_x must be comparable with β_y (since β_x is the minimal element of γ that is incomparable with β_y), but if $\alpha \ni \beta_y$ or $\alpha = \beta_y$ then β_y would be comparable with β_x, so we must have $\alpha \in \beta_y$.
The same argument shows that $\alpha \in \beta_y \to \alpha \in \beta_x$, but then $\beta_x = \beta_y$. Thus there are no incomparable elements in γ.

Transitive: Since every element of γ is a transitive set.

Well-founded: Since $\in$ is well-founded on any set (by the axiom of foundation).

... so $(\gamma, \in)$ is a well-ordered set. Thus if we define $\alpha < \beta$ by $\alpha \in \beta$, then each ordinal is by definition the well-ordered set of all smaller ordinals.

4.3 Successor and limit ordinals

Given an ordinal α, what is the smallest ordinal β such that $\alpha < \beta$? By definition we must have $\alpha \in \beta$, and then also $\alpha \subseteq \beta$ since β is a transitive set. The smallest set that has α both as an element and as a subset is

$$\beta = S(\alpha) = \alpha \cup \{\alpha\}.$$

This is a set of ordinals, and it is transitive since

$$x \in y \in \alpha \to x \in \alpha$$
$$x \in y \in \{\alpha\} \to x \in \alpha$$

so it is itself an ordinal. Thus $S(\alpha)$ is the "next" ordinal after α, or the *sucessor* of α.

The natural numbers can all be generated from 0 by repeated application of the successor function. In other words, each natural number is either 0 or a successor of some other natural number (this is essentially the meaning of the axiom schema of induction). But this is not the case for infinite ordinals.

Example 9. There is no ordinal α such that $S(\alpha) = \omega$, since ω is an infinite set of finite sets, and $\alpha \cup \{\alpha\}$ is either finite (if α is finite) or it contains an infinite set (if α is infinite).

Ordinals that are not successors are called *limit ordinals*.[3]

4.4 Least upper bounds and order types

Given a set X of ordinals, what is the least ordinal β such that $\alpha \leq \beta$ for all $\alpha \in X$? We have that $\alpha \leq \beta$ if and only if $\alpha \subseteq \beta$, and the smallest set containing all elements of X as subsets is $\cup X$. This is a set of ordinals, and it is transitive since

$$a \in b \in \cup X \ \to \ a \in b \in \alpha \in X \ \to \ a \in \alpha \in X \ \to \ a \in \cup X$$

so it is itself an ordinal. We say that $\cup X$ is the *least upper bound* of the set X.

Example 10. The least upper bound of the set $\{1, 2, 4, 8, 16 \ldots\}$ is ω.

We previously showed that $\in$ is trichotomous on any specific ordinal γ. Now, given any pair of ordinals α and β, we can easily construct an ordinal $\gamma = S(\alpha) \cup S(\beta)$ that contains both α and β. Thus all ordinals are comparable, and $\in$ is a well-ordering on the whole class of ordinals Ω.

Lemma 5. *If two ordinals are not equal, then one of them is an initial segment of the other.*

Proof. Since they are comparable but not equal, one is an element of the other, and if $\alpha \in \beta$ then $\alpha = \beta_{<\alpha}$. □

[3]Often 0 is not considered a limit ordinal, but we include it: under this definition, limit ordinals are precisely those ordinals λ that satisfy $\cup\lambda = \lambda$.

Thus, we have

$$\alpha < \beta \;\leftrightarrow\; \alpha \in \beta \;\leftrightarrow\; \alpha \subsetneq \beta$$

and we can use these relations interchangeably. Another consequence is that if two ordinals are isomorphic as well-ordered sets, they are equal (otherwise a well-ordered set would be isomorphic to an inital segment of itself). Thus a well-ordered set X can be isomorphic to at most one ordinal α. If such an α exists, we write $\mathrm{ord}(X) = \alpha$ and say that X is of *order type* α. Next we show that every well-ordered set has an order type. Since every well-ordered set is an initial segment of some other well-ordered set, it suffices to prove the following:

Theorem 1. *Every initial segment of a well-ordered set is order-isomorphic to an ordinal.*

Proof. Let W be any well-ordered set and suppose that

$$\{\, x \in W \mid W_{<x} \text{ is not isomorphic to any ordinal} \,\}$$

is non-empty. Then it has a smallest element m, and $\mathrm{ord}(w)$ is defined for all $w < m$: we use this to construct $\{\, \mathrm{ord}(w) \mid w \in W_{<m} \,\}$. This is a transitive set of ordinals and therefore an ordinal α. But now $W_{<m} \cong_{\mathrm{ord}} \alpha$, contradicting the fact that $W_{<m}$ is not isomorphic to any ordinal. □

4.5 Transfinite induction and recursion

A standard (finite) induction proof of a statement $P(n)$ ranging over the natural numbers consists of two parts: proving the base case $P(0)$, and proving the inductive step $P(n) \to P(S(n))$. But such a proof does not work on the ordinals, since there are ordinals that are neither zero nor successors. Instead we have the principle of *transfinite* induction (see [1] p. 206):

Theorem 2. *To prove a statement $P(\alpha)$ for all ordinals α, it suffices to:*

1. *Prove $P(0)$*
2. *Prove $P(\alpha) \to P(S(\alpha))$*
3. *Prove that if λ is a non-zero limit ordinal, and $P(\gamma)$ holds for every $\gamma \in \lambda$, then $P(\lambda)$ holds.*

Another way to say this is that when we are trying to prove $P(\beta)$, we can assume $P(\alpha)$ for all $\alpha \in \beta$. Transfinite *recursion* works similarly: when defining $f(\beta)$, we can use $f(\alpha)$ for all $\alpha \in \beta$. This is similar to the construction we used in the proof of theorem 1, where we exploited the fact that we could assume the function ord to be defined on all "smaller" initial segments.

4.6 Ordinal arithmetic

We now extend the recursive definitions for arithmetic on natural numbers to ordinals, by simply adding a third case for non-zero limit ordinals λ:

$$\begin{array}{ccc} \alpha + 0 := \alpha & \alpha \cdot 0 := 0 & \alpha^0 := 1 \\ \alpha + S(\beta) := S(\alpha + \beta) & \alpha \cdot S(\beta) := (\alpha \cdot \beta) + \alpha & \alpha^{S(\beta)} := (\alpha^\beta) \cdot \alpha \\ \alpha + \lambda := \bigcup_{\gamma \in \lambda} \alpha + \gamma & \alpha \cdot \lambda := \bigcup_{\gamma \in \lambda} \alpha \cdot \gamma & \alpha^\lambda := \bigcup_{\gamma \in \lambda} \alpha^\gamma \end{array}$$

This transfinite recursive definition of ordinal arithmetic is compatible with our earlier definition of arithmetic on well-ordered sets, in the sense that

$$\begin{aligned} \mathrm{ord}(A) + \mathrm{ord}(B) &= \mathrm{ord}(A + B) \\ \mathrm{ord}(A) \cdot \mathrm{ord}(B) &= \mathrm{ord}(A \cdot B) \\ \mathrm{ord}(A)^{\mathrm{ord}(B)} &= \mathrm{ord}(A^B) \end{aligned}$$

for all well-ordered sets A and B (see [1] pp. 220, 225). Thus our examples showing that addition and multiplication are not commutative can be directly translated into ordinal arithmetic:

$$\begin{array}{cc} \mathbf{1} + \mathbb{N} \cong \mathbb{N} \ncong \mathbb{N} + \mathbf{1} & \mathbb{N} \cdot \mathbf{2} \cong \mathbb{N} + \mathbb{N} \ncong \mathbb{N} \cong \mathbf{2} \cdot \mathbb{N} \\ 1 + \omega = \omega \neq \omega + 1 & \omega \cdot 2 = \omega + \omega \neq \omega = 2 \cdot \omega \end{array}$$

We now state some other basic properties of ordinal arithmetic (for proofs of these properties, see for instance [1]). Both addition and multiplication are associative:

$$\begin{aligned} \alpha + (\beta + \gamma) &= (\alpha + \beta) + \gamma \\ \alpha \cdot (\beta \cdot \gamma) &= (\alpha \cdot \beta) \cdot \gamma \end{aligned}$$

so we can write sums and products without parentheses, as we are used to. We can distribute operations from the left but not from the right:

$$\begin{array}{cc} \alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma) & \alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma \\ (\omega + 1) \cdot \omega \neq (\omega \cdot \omega) + (1 \cdot \omega) & (\omega \cdot 2)^\omega \neq \omega^\omega \cdot 2^\omega \end{array}$$

All of the operations are monotone in the right argument: if $\alpha < \beta$, then

$$\begin{array}{cc} \gamma + \alpha < \gamma + \beta & \\ \gamma \cdot \alpha < \gamma \cdot \beta & (\gamma > 0) \\ \gamma^\alpha < \gamma^\beta & (\gamma > 1) \end{array}$$

What will be specifically useful for us, is that if $\alpha < \beta$, then

$$\omega^\alpha \cdot k < \omega^\alpha \cdot \omega = \omega^{S(\alpha)} \leq \omega^\beta$$

for any natural number k, from which it follows that

$$\sum_{i=1}^{n} \omega^{\alpha_i} k_i < \bigcup_{i=1}^{n} \alpha_i$$

for any natural numbers k_i and ordinals α_i.

The arithmetic operations also allow a new characterization of limit and successor ordinals: Every ordinal can be uniquely represented as $\gamma = \omega \cdot \alpha + k$ with k a natural number, and γ is a limit ordinal precisely when $k = 0$.

5 Proving Goodstein's theorem

5.1 Moving to an infinite base

Recall that the operation $(m)_{n \to k}$ takes the complete base-n represenation of m and changes every occurence of n to k. We now extend this notation to allow k to be the ordinal number ω. For example:

$$\begin{aligned}
100_{6\to\omega} &= (6^2 \cdot 2 + 6 \cdot 4 + 4)_{6\to\omega} = \omega^2 \cdot 2 + \omega \cdot 4 + 4 \\
100_{3\to\omega} &= (3^{3+1} + 3^2 \cdot 2 + 1)_{3\to\omega} = \omega^{\omega+1} + \omega^2 \cdot 2 + 1 \\
100_{2\to\omega} &= (2^{2^2+2} + 2^{2^2+1} + 2^2)_{2\to\omega} = \omega^{\omega^\omega+\omega} + \omega^{\omega^\omega+1} + \omega^\omega
\end{aligned}$$

Since we have defined the operations of addition, multiplication and exponentiation on ordinals, these expressions are all valid ordinal numbers. Here we see why we must write the terms in decreasing order, and coefficients to the right: otherwise terms and coefficients might be "absorbed" since $1 + \omega = \omega$ and $2 \cdot \omega = \omega$.

The motivation for introducing this operation is that by moving from a natural number base to the infinite ordinal base ω, we can nullify the effects of increasing the base. For instance:

$$(3^{3\cdot 2} + 1)_{3\to\omega} = (4^{4\cdot 2} + 1)_{4\to\omega} = \omega^{\omega\cdot 2} + 1$$

Let's convince ourselves that this works in general.

Lemma 6. *For all natural numbers $m, n, k > 1$ such that $n < k$:*

$$(m_{n\to k})_{k\to\omega} = m_{n\to\omega}$$

Proof. To calculate the left hand side, we start with the complete base-n representation of m, and replace every occurence of n with k. Since $n < k$, the expression we then have is already in complete base-k. Thus we can directly replace every occurence of k with ω. Since there are no k:s in the complete base-n representation of m (again since $n < k$), the ω:s in the final expression correspond precisely to the n:s in the original expression. □

This property inspires us to make the following definition:

$$D_n(m) := G_n(m)_{n \to \omega}$$

The idea is that each Goodstein sequence has a corresponding sequence of ordinal numbers; and that the sequence of ordinals is not affected by the "increase the base"-step, but only by the "decrease the number"-step.

5.2 A closer analysis of a Goodstein sequence

To develop a feel for what is happening with D_n, let's compare $G_n(4)$ with its corresponding ordinal sequence $D_n(4)$:

n	G_n	D_n
2	2^2	ω^ω
3	$3^2 \cdot 2 + 3 \cdot 2 + 2$	$\omega^2 \cdot 2 + \omega \cdot 2 + 2$
4	$4^2 \cdot 2 + 4 \cdot 2 + 1$	$\omega^2 \cdot 2 + \omega \cdot 2 + 1$
5	$5^2 \cdot 2 + 5 \cdot 2$	$\omega^2 \cdot 2 + \omega \cdot 2$
6	$6^2 \cdot 2 + 6 + 5$	$\omega^2 \cdot 2 + \omega + 5$
7	$7^2 \cdot 2 + 7 + 4$	$\omega^2 \cdot 2 + \omega + 4$
8	$8^2 \cdot 2 + 8 + 3$	$\omega^2 \cdot 2 + \omega + 3$
9	$9^2 \cdot 2 + 9 + 2$	$\omega^2 \cdot 2 + \omega + 2$
10	$10^2 \cdot 2 + 10 + 1$	$\omega^2 \cdot 2 + \omega + 1$
11	$11^2 \cdot 2 + 11$	$\omega^2 \cdot 2 + \omega$
12	$12^2 \cdot 2 + 11$	$\omega^2 \cdot 2 + 11$

Notice how the ordinal numbers capture the "shape" of the complete base-n representations, without getting distracted by the size of the base n. For instance, from D_6 to D_{11}, most of the expression remains constant while the last term decreases. In general, if $D_n = \omega \cdot \alpha + k$, then $D_{n+k} = \omega \cdot \alpha$. We can use this to skip ahead faster in the table:

n	G_n	D_n
$23 = 12 + 11$	$23^2 \cdot 2$	$\omega^2 \cdot 2$
$24 = 3 \cdot 2^3$	$24^2 + 24 \cdot 23 + 23$	$\omega^2 + \omega \cdot 23 + 23$
$\vdots$	$\vdots$	$\vdots$
$47 = 24 + 23$	$47^2 + 47 \cdot 23$	$\omega^2 + \omega \cdot 23$
$48 = 3 \cdot 2^4$	$48^2 + 48 \cdot 22 + 47$	$\omega^2 + \omega \cdot 22 + 47$
$\vdots$	$\vdots$	$\vdots$
$95 = 48 + 47$	$95^2 + 95 \cdot 22$	$\omega^2 + \omega \cdot 22$
$96 = 3 \cdot 2^5$	$96^2 + 96 \cdot 21 + 95$	$\omega^2 + \omega \cdot 21 + 95$

We notice that so far, D_n is a limit ordinal precisely when n is of the form $3 \cdot 2^k - 1$. This pattern will continue, since the transition from one limit ordinal to the next always looks like this ...

n	D_n
p	$\omega \cdot \alpha$
$p+1$	$\omega \cdot \alpha' + p$
$\vdots$	$\vdots$
$2p+1$	$\omega \cdot \alpha''$

... and if $p = 3 \cdot 2^k - 1$, then $2p + 1 = 3 \cdot 2^{k+1} - 1$. Thus we can easily make a table showing only the limit ordinals in the sequence:

k	$D_{3\cdot 2^k-1}$
0	ω^ω
1	$\omega^2 \cdot 2 + \omega \cdot 2$
2	$\omega^2 \cdot 2 + \omega$
3	$\omega^2 \cdot 2$
4	$\omega^2 + \omega \cdot 23$
5	$\omega^2 + \omega \cdot 22$
6	$\omega^2 + \omega \cdot 21$
7	$\omega^2 + \omega \cdot 20$

Notice that if $D_{3\cdot 2^k-1} = \omega^2 \cdot \alpha + \omega \cdot l$, then $D_{3\cdot 2^{k+l}-1} = \omega^2 \cdot \alpha$. We only need to skip ahead like this two times before the sequence terminates:

k	$D_{3\cdot 2^k-1}$
4	$\omega^2 + \omega \cdot 23$
$\vdots$	$\vdots$
$4 + 23$	ω^2
28	$\omega \cdot (3 \cdot 2^{27} - 1)$
$\vdots$	$\vdots$
$28 + 3 \cdot 2^{27} - 1$	0

So $D_n(4)$ and $G_n(4)$ terminate at the base

$$n = 3 \cdot 2^k - 1 = 3 \cdot 2^{27+3\cdot 2^{27}} - 1$$

Note that while we used ordinal numbers D_n here, we could have come to the same conclusion by looking directly at the complete base-n representation of G_n instead, although the expressions involved are then a bit messier. Another way of analysing this sequence, without any reference to ordinals, can be found in [3] p. 205. This highlights the importance of the universal quantifier in Goodstein's theorem. While the statement

$$\forall m \, \exists n \, (G_n(m) = 0)$$

"Every Goodstein sequence terminates"

is not provable in PA, there is nothing stopping us from proving it for some specific value of m:

$$\exists n \, (G_n(4) = 0)$$

"The Goodstein sequence starting at 4 terminates"

5.3 One last lemma

We now have a clear path to prove Goodstein's theorem: simply show that D_n is always a decreasing sequence of ordinals. The only missing piece is the following lemma: when we decrease a number (written in some base n), its corresponding ordinal number representation also decreases.

Lemma 7. *For all natural numbers $a, n > 1$:*

$$(a-1)_{n\to\omega} < (a)_{n\to\omega}$$

Proof. Since only the smallest power of n in the complete base-n representation of a is affected when we subtract 1, it suffices to prove

$$(n^k - 1)_{n\to\omega} < (n^k)_{n\to\omega}.$$

Letting $c = n - 1$, and assuming (by induction on the "height of the representation") that what we are trying to prove holds true for the exponents:

$$(n^k - 1)_{n\to\omega} = (n^{k-1}c + n^{k-2}c + \cdots + nc + c)_{n\to\omega} =$$
$$= \omega^{(k-1)_{n\to\omega}}c + \omega^{(k-2)_{n\to\omega}}c + \cdots + \omega c + c \leq \omega^{k_{n\to\omega}} = (n^k)_{n\to\omega}$$

□

Now we are finally ready to prove Goodstein's theorem.

Theorem 3 (Goodstein's theorem)**.** *The Goodstein sequence defined by*

$$G_2 := m$$
$$G_{n+1} := (G_n)_{n\to n+1} - 1$$

always terminates, regardless of the value of m.

Proof. If we let

$$D_n = (G_n)_{n\to\omega}$$

then

$$D_{n+1} = ((G_n)_{n\to n+1} - 1)_{n+1\to\omega} < ((G_n)_{n\to n+1})_{n+1\to\omega} = (G_n)_{n\to\omega} = D_n$$

so D_n is a decreasing chain of ordinals. Thus D_n, and therefore also G_n, must terminate in a finite number of steps.

□

Appendices

A First-order logic

A *theory* in first-order logic consists of a universe of discourse, some functions and predicates of different arities, and a collection of axioms.

Terms are expressions that range over values in the domain of discourse.

- If x is a variable, then x is a term.
- If f is a n-ary function and $t_1, t_2, \ldots t_n$ are terms, then $f(t_1, \ldots, t_n)$ is a term.

Formulas are statements about the universe of discourse.

- If P is a n-ary predicate, and $t_1, t_2, \ldots t_n$ are terms, then $P(t_1, t_2, \ldots, t_n)$ is a formula.
- If φ and ψ are formulas and x is a variable, then the following are formulas:

$\neg\varphi$	not φ
$\varphi \wedge \psi$	φ and ψ
$\varphi \vee \psi$	φ or ψ
$\varphi \to \psi$	φ implies ψ
$\forall x(\varphi)$	for all x, φ
$\exists x(\varphi)$	for some x, φ

Notice that formulas may only be quantified over variables. For instance, the following is not a first-order formula:

$$\forall\varphi(\varphi \to \varphi)$$

In spite of this, we sometimes want to take an expression like the above as an axiom. In such a case we postulate an *axiom schema* instead of a single axiom; namely, an infinite set of axioms, one for every possible formula φ.

We also include as part of the logic the binary equality predicate $=$ as well as some basic axioms about it, stating that every variable is equal to itself, and that if two variables are equal they may be freely interchanged both in functions and in formulas.

A.1 Deductive systems

A first order theory cannot do much by itself; we also need some way to deduce new truths from the axioms. There are multiple such deductive systems one can use. A theoretically beautiful one is the Hilbert-style system where we add a number of logical axiom schemas, and then prove theorems using the single rule of interference of modus ponens:

> From φ and $\varphi \to \psi$, deduce ψ.

A deductive system that is closer to how we normally think about proofs is natural deduction. There we do not use any logical axioms, but instead introduce inference rules for all the different logical operators, such as:

> From φ and ψ, deduce $\varphi \wedge \psi$.

In both cases, some care must be taken to handle quantifiers correctly. It becomes necessary to distinguish between *free* and *bound* occurences of variables to know when we can perform substitutions and generalizations.

A.2 Extension by definition

Under which circumstances can we safely extend a first order theory with new functions and predicates? Given any formula φ with free variables among x_1, x_2, $\dots$ x_k we can add a new predicate P to the signature, along with the axiom:

$$\varphi(x_1, \dots, x_k) \leftrightarrow P(x_1, \dots, x_k)$$

Similarly, if $\psi(x_1, x_2, \dots x_k, y)$ is a formula such that for any choice of the variables x_i, there is exactly one choice of y such that the formula is true, we can add a new function f to the signature, along with the axiom

$$\psi(x_1, x_2, \dots x_k, f(x_0, x_1, \dots x_k))$$

Then every statement in the new theory can be translated back into the old theory, and a statement is provable in the new theory if and only if its translation is provable in the old theory.

B Some more set theory

B.1 Consequences of replacement

Lemma 8 (Separation)**.**

$$\forall X\, \exists Y (x \in Y \leftrightarrow x \in X \wedge \psi(x))$$

For any set X and unary predicate ψ, we can construct the set $\{x \in X \mid \psi(x)\}$.

Proof. Use the axiom schema of replacement with $\varphi(x, y) :\Leftrightarrow [(x = y) \wedge \psi(x)]$. □

Lemma 9 (Empty set)**.**

$$\exists X (\forall y\, (y \notin X))$$

There is a (unique, by extensionality) empty set.

Proof. Use separation with some predicate that is always false (such as $\psi(x) :\Leftrightarrow (x \in x)$) on any set (the axiom of infinity guarantees that there is at least one set). □

Lemma 10 (Singletons)**.**

$$\forall a\, \exists X [x \in X \leftrightarrow x = a]$$

For all sets a, there is a set $\{a\}$.

Proof. Use the axiom schema of replacement on any non-empty set with $\varphi(x, y) :\Leftrightarrow (y = a)$. □

Lemma 11 (Pairs)**.**

$$\forall a\, \forall b\, \exists X [x \in X \leftrightarrow (x = a \vee x = b)]$$

For all sets a, b, there is a set $\{a, b\}$.

Proof. Use the axiom schema of replacement on $\mathcal{P}(\mathcal{P}(\varnothing)) = \{\varnothing, \{\varnothing\}\}$ with $\varphi(x, y) :\Leftrightarrow (x = \varnothing \wedge y = a) \vee (x = \{\varnothing\} \wedge y = b)$. □

B.2 The cumulative hierarchy

The cumulative hierarchy is a transfinite sequence of sets defined by:

$$\begin{aligned} V_0 &:= \varnothing \\ V_{S(\alpha)} &:= \mathcal{P}(V_\alpha) \\ V_\lambda &:= \bigcup_{\gamma \in \lambda} \gamma \end{aligned}$$

or, equivalently:

$$V_\beta := \bigcup_{\alpha \in \beta} \mathcal{P}(V_\alpha)$$

Thus

$$\begin{aligned} V_1 &= \mathcal{P}(V_0) = \{\varnothing\} \\ V_2 &= \mathcal{P}(V_1) = \{\varnothing, \{\varnothing\}\} \\ V_3 &= \mathcal{P}(V_2) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\} \\ &\vdots \\ V_\omega &= \bigcup_{n \in \omega} V_n \end{aligned}$$

V_ω is the set of all *hereditarily finite sets*, and it is a model for the theory $\mathsf{ZF} - \mathsf{Infinity}$.

$$\begin{aligned} V_{\omega+1} &= \mathcal{P}(V_\omega) \\ V_{\omega+2} &= \mathcal{P}(\mathcal{P}(V_\omega)) \\ &\vdots \\ V_{\omega+\omega} &= V_\omega \cup \mathcal{P}(V_\omega) \cup \mathcal{P}(\mathcal{P}(V_\omega)) \ldots \end{aligned}$$

$V_{\omega+\omega}$ is a model of Zermelo set theory (an earlier version of ZF, without foundation and replacement). It can be thought of as the universe of "ordinary mathematics": for instance, already in $V_{\omega+2}$ we can construct the real numbers. While each V_α is a set, if we take the union over all the ordinals we end up with the proper class V:

$$\bigcup_{\alpha \in \Omega} V_\alpha = V$$

i.e. for each set x there is some ordinal α such that $x \in V_\alpha$ (see [1] p. 227 for a proof). If α is the smallest such ordinal, we say that α is the *rank* of x and write $R(x) = \alpha$. We can calculate the rank of a set like this:

$$R(X) = \bigcup_{x \in X} S(R(x))$$

In particular, the rank of an ordinal number is itself:

$$R(\alpha) = \alpha$$

and each V_α is the set of all sets with rank less than α:

$$V_\alpha = \{x \mid R(x) < \alpha\}$$

Notice that if $x \in y$, then $R(x) < R(y)$. This gives us a straightforward way to construct an infinite ordinal from our axiom of infinity

$$\exists X \neq \varnothing \;\; \forall a \in X \;\; \exists b \in X \;\; a \in b$$

which guarantees the existence of a set X containing an infinite ascending chain

$$x_0 \in x_1 \in x_2 \in x_3 \ldots$$

which must then satisfy

$$R(x_0) < R(x_1) < R(x_2) < R(x_3) \ldots .$$

Since $R(X) > R(x_i)$ for each i, it follows that $R(X)$ is an infinite ordinal. In particular, $\omega \subseteq R(X)$.

References

[1] Derek Goldrei. *Classic Set Theory.* Chapman & Hall, 1996.

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

[3] Julian Havil. *Impossible?* Princeton University Press, 2008.

[4] Thomas Jech. *Set Theory.* Springer, 2003.

[5] Laurie Kirby and Jeff Paris. Accessible independence results for peano arithmetic. *Bulletin of the London Mathematical Society*, 14(4):285–293, 1982.

[6] John Stillwell. *Roads to Infinity.* CRC Press, 2010.