ON RESULTS PROVABLE WITH ORDINALS BUT UNPROVABLE WITH PEANO ARITHMETIC

OWEN JIANG

ABSTRACT. Peano arithmetic, despite its logical rigor and solid first-order axioms, was found to be unable to prove necessarily true statements. Ordinal arithmetic, a second-order logical system, goes beyond Peano arithmetic and can prove certain true statements that cannot be proven under Peano arithmetic. This paper will start with a brief introduction to ordinals and how they are derived from cardinals, then go on to discuss two such ordinal proofs: Gentzen's consistency proof, which used primitive recursive arithmetic and transfinite induction to prove Peano arithmetic, and Goodstein's theorem, where Goodstein famously proved how Goodstein sequences will always terminate at 0. For each proof, we end with a brief summary of the novel ways in which ordinals were employed to prove the results from these three scenarios. We finish with a brief note on the motivations for employing ordinal arithmetic in problems in math and an analysis of what ordinals can offer that Peano arithmetic cannot.

1. Introduction

The mathematician David Hilbert, a proponent of mathematical formalism, was heavily interested in proving mathematics' completeness, consistency, and decidability. One system of arithmetic that was used to build up mathematics from the ground-up using first-order logic was Peano arithmetic, using fifteen Peano axioms that were viewed as self-evident. Despite Hilbert's grand and hopeful vision of a theory of math rooted in formal logic, numerous contradictions arose in the following years. Most notably, Kurt Gödel, with his incompleteness proofs, proved that there will always be statements in a formal mathematics system that cannot be proved or disproved (meaning the system is incomplete). While Gödel has the greatest notability in terms of demonstrating the limitations of Peano arithmetic, other mathematicians have made similar ventures, and some notably used ordinal arithmetic as a method for proving various theorems and problems that were proven to be unprovable under Peano arithmetic. This paper will begin with a brief discussion of cardinals and ordinals and will further discuss two such proofs and theorems pertaining to ordinal proofs: Gentzen's consistency proof and Goodstein's theorem. A final discussion will include the significance of ordinal proofs.

2. What are ordinals?

2.1. **Cardinals and counting.**

Cardinals are used in mathematics to count the number of numbers in a set. For example, Figure 1 shows four ducks in the upper set.

Definition 2.1 (Cardinality)**.** The *cardinality* of a set S is the number of distinct elements in that set S.

Date: July 11th, 2023.

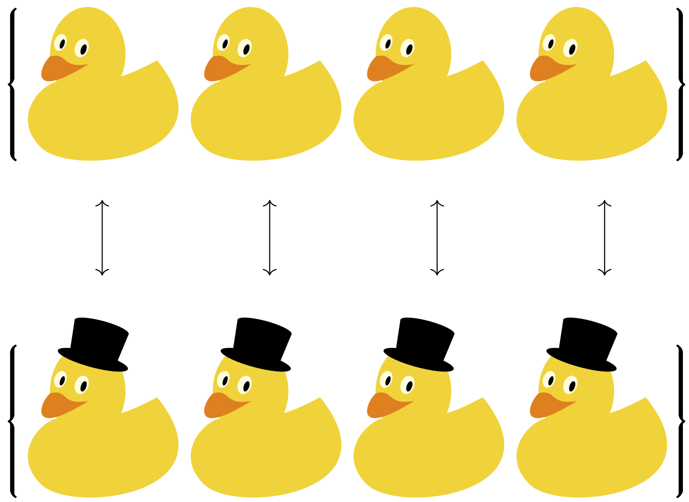

Figure 1. The cardinality of the set of four ducks with no top hats is 4, as the cardinality of the set of four ducks with top hats is also 4.

The cardinality of the top set in Figure 1 is 4, because there are four elements in the set. If we compare the top and bottom sets, the number of ducks in each set is the same because there is a bijection (a one-to-one correspondence) between each duck with no top hat and each duck with a top hat.

One interesting consequence of this can be seen when we extend the idea of cardinality to various sizes of infinity. The cardinality of the set of natural numbers (that is, the set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$) is known as $\aleph_0$ (pronounced aleph-null), the first infinite cardinal.

Definition 2.2 (Infinite countable set)**.** A set S is *countably infinite* if and only if it has the same cardinality as the set of natural numbers $\mathbb{N}$. Any countably infinite set must have cardinality $\aleph_0$.

Using this definition, we can found numerous other countably infinite sets. Take the set of all integers $\mathbb{Z}$. We can have a bijection shown below in Table 1.

$\mathbb{N}$	0	1	2	3	4	$\cdots$	n_k
$\mathbb{Z}$	0	-1	1	-2	2	$\cdots$	$(-1)^{n_k} \cdot \lceil n_k/2 \rceil$

Table 1. The set of natural numbers $\mathbb{N}$ and integers $\mathbb{Z}$ have the same cardinality $\aleph_0$.

As shown in the table, each n_k in the natural numbers maps to exactly one integer in the total set of the integers. The fact that all of the natural numbers are present in the set of integers $\mathbb{Z}$ does not matter in this case, the ability to perform a bijection is how we compare the "sizes" of two sets.

2.2. **Ordinals and ordering.** While cardinals are involved in the counting of the elements of a set, ordinals are involved in the ordering of the elements of a set. In Figure 2, we have an infinite number of sticks getting smaller and smaller, and if we presume that there are countably infinitely many sticks to the right, each smaller than the last, then the cardinality of these sticks is the same as the natural numbers, as we can label each one with a natural number.

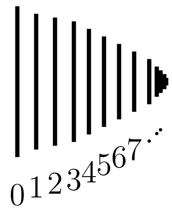

Figure 2. The cardinality of these sticks is $\aleph_0$.

What happens when we add one more long stick at the end, as in Figure 3? The cardinality of the set remains $\aleph_0$, as we can number the right one with 0 first and then continue in sequential order from the leftmost stick and going right towards infinity.

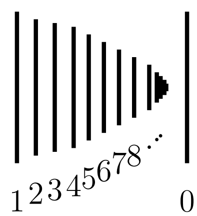

Figure 3. The cardinality of these sticks is *still* $\aleph_0$.

Definition 2.3 (Ordinal)**.** An *ordinal* is a positional cardinal number assigned to describe the position of an item in a set relative to other elements. Ordinals can be extended to be allowed to enumerate infinite sets.

In English, we order things with words like "first", "second", and "kth".

It's important to note at this point that while we use the cardinal numbers as ordinals, they are not the same thing. Cardinal numbers tell us the number of elements of a set, while ordinal numbers tell us the order in which the elements appear. When we talk about infinite cardinals and ordinals, we start using the $\aleph$ numbers for cardinals and the ω numbers for ordinals.

Returning to our stick example, if we assign an ordinal to each stick in Figure 3 by the order that they appear from left to right, forcing ourselves to start with 0 on the left, we can assign the last stick on the right the smallest infinite ordinal ω (omega), as shown in Figure 4.

Notice that if we had ordered the sticks the same way that we ordered them with cardinals, the infinite ordinal ω would never be used.

Definition 2.4 (Totally ordered)**.** A set S is defined to be *totally ordered* and is written $(S, \leq)$ if every element of S can be compared with every other element of S. That is, there exists some clearly-defined property for every element α in S that allows a clear two-choice comparison (before or after, greater or smaller, preceding or succeeding, etc.), between α and every other element in S.

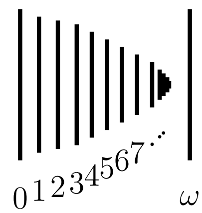

Figure 4. The cardinality of these sticks is *still* $\aleph_0$, even though we have ordered the set in a different way.

Using this definition for ordinals, we can define a method of comparison as follows: an ordinal α precedes an ordinal β if α is used to order elements before β.

Definition 2.5 (Well-ordered set)**.** A set S is defined to be *well-ordered* if it satisfies both of the following two properties:

(1) S is totally ordered (all elements in S are comparable with each other; this is often denoted as $(S, \leq)$).
(2) Every nonempty subset of S has a least element.

For example, the set of integers $\mathbb{Z}$ is not *well-ordered* because it has no least element: there is no least integer, as you can always find a negative number less than any one you have currently thought of.

At this point, a good definition of how we compare ordinals in totally ordered sets is in order.

Definition 2.6 (Order type)**.** Two well-ordered sets A and B have the same *order type* if they are order-isomorphic—there exists a bijection $A \to B$ that orders A and B with the same ordinals such that the bijection and its inverse are monotonic (order-preserving).

In practice, the most critical part of this definition is the bijection.

We assign order types to various well-ordered sets using the next ordinal which is not already in the set. For example, the set of natural numbers $\mathbb{N}$ has order type ω, as ω is the ordinal that succeeds the ordering of all the natural numbers in $\mathbb{N}$ (this is called the *supremeum*). Take Figure 5 below.

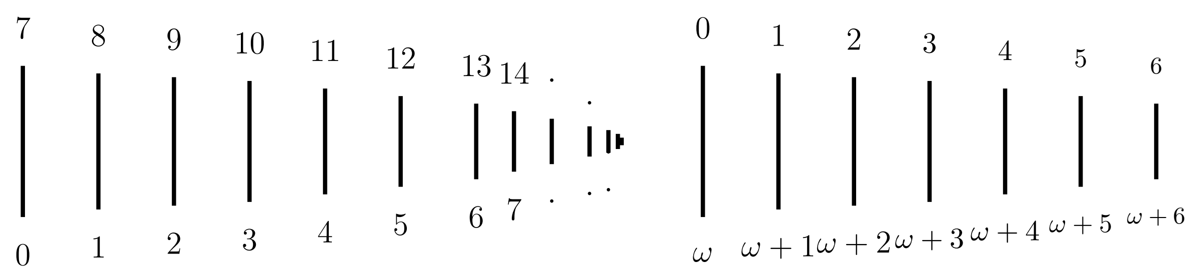

Figure 5. The numbers above each stick are the cardinals assigned to each stick. The cardinality of the sticks is *still* $\aleph_0$. The numbers below each stick are the ordinals assigned to each stick. The order type of this set is $\omega + 7$.

The order type of the set shown above is $\omega + 7$ because the ω describes the ordering of the first $\aleph_0$ sticks, and there are 7 sticks succeeding that: from ω to $\omega + 6$.

Let us imagine an $\aleph_0$ number of sticks instead of just 7, all occurring after the first $\aleph_0$ sticks with the same order type as $\mathbb{N}$, as in Figure 6.

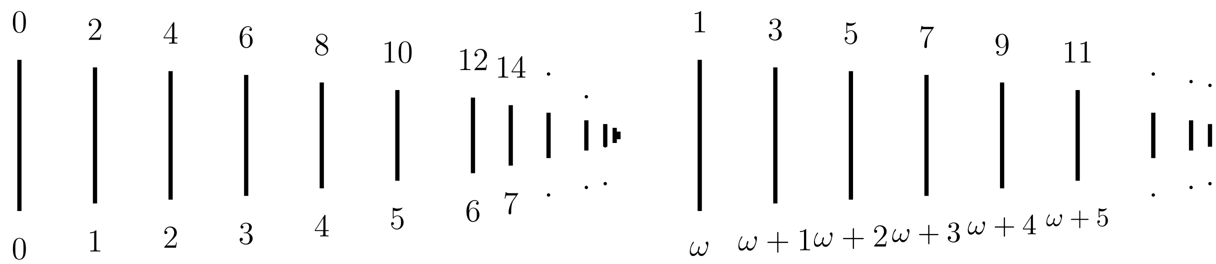

Figure 6. The numbers above each stick are the cardinals assigned to each stick. The cardinality of the sticks is actually *still* $\aleph_0$, because we can count the countably infinite number of sticks on the left with even natural numbers and the countably infinite number of sticks on the right with odd natural numbers. The numbers below each stick are the ordinals assigned to each stick. The order type of this set is $\omega * 2$.

We can continuously construct more and more countably infinite numbers of sticks to the right using the axiom schema of replacement.

Definition 2.7 (Axiom Schema of Replacement)**.** For any set S, the image of S under any mapping is also itself a set.

While the words "image" and "mapping" are defined more clearly under ZF set theory, we can apply this method of creating more ordinals farther to the "right" of the ones we have defined by creating a function that duplicates the ordinals from ω to some higher ordinal, and giving them a new name since they are distinct from the previous ordinals. Repeatedly mapping the sticks ordered ω to right before $\omega * 2$ can get us to $\omega * \omega$ (also known as ω^2) and eventually ω^ω. The limit of the expression $\omega^{\omega^{\omega^{\cdots}}}$ is called ε_0 (read as epsilon-nought), which is still countable and has cardinality $\aleph_0$. (The reader is encouraged to use the previous figures as hints to ponder on the reasoning for this and the manner in which we can count through an ε_0-ordered number of sticks.) While it is possible to find ever higher ordinals, they are unnecessary for understanding the three proofs presented in this paper.

We may find it useful to use one more definition.

Definition 2.8. The *natural sum* of two ordinals, denoted $\alpha \# \beta$, is defined to be the sum of all the individual ω terms in both α and β upon reordering all the terms of the two ordinals together by decreasing size (this is to combat the non-commutativity of ordinal addition).

For example, if $\alpha = \omega^{\omega+1} + 1$ and $\beta = \omega^{\omega^{\omega^{\omega^3+1}}} + \omega^{\omega+1} + \omega$, then $\alpha \# \beta = \omega^{\omega^{\omega^3+1}} + \omega^{\omega+1} + \omega^{\omega+1} + \omega + 1$. Notice that if $\alpha \# \beta$ had been rearranged in reverse order, the result would be just the term with the highest magnitude, $\omega^{\omega^{\omega^3+1}}$.

In order to decide properties of ordinals, especially infinite ones, a helpful tool is *transfinite induction*, a tool that Gentzen used for his consistency proof.

Theorem 2.9 (Correctness of transfinite induction)**.** *Let some property $P(\alpha)$ be defined for all ordinals α, and for all ordinals $\beta < \alpha$, let $P(\beta)$ is true for all such β. If $P(\lambda)$ is true for* *some limit ordinal λ, given that $P(\beta)$ is true for all $\beta < \lambda$, then P is a property that must hold for all ordinals.*

This theorem is presumed to be correct under ZFC. An example of its use is as follows.

Let us define the property P as "accessibility", our ability to define the ordinal, and let us order with decimal ordinals starting with 0.1. Let us ignore how we generally order things with natural numbers, a decimal-point ordering system is equally valid in this system. We can go through the ordinals as follows: $0.1, 0.2, 0.3, \ldots, 0.9, 0.11, 0.12, \ldots, 0.19, 0.111, \ldots$. In this way, we can hit every single decimal number between 0 and 1. Next, let us presume that the accessibility of all numbers up to a certain ordinal η have been proved, and we now need to prove the accessibility of $\eta + 1$. The first of the "$\eta + 1$ ordinals" with the "1" digit in the first decimal place is accessible. For every ordinal ordered before this ordinal, assume they satisfy a property P, and for every one of these ordinals $\alpha < \eta + 1$, there is a set B that contains $\alpha + 1$ of the numbers with a property $P + 1$, which is an isomorphism of the set A of numbers ordered before $\alpha + 1$ with the property $P + 1$. Ordering through these specific $P + 1$ numbers is exactly isomorphic to ordering the set of ordinals α with the property P. As a certain $\eta + 1$ becomes accessible, all the numbers in the set of $\alpha < \eta + 1$ also become *accessible*. Thus, we can order this set B exactly how we already ordered the set A, and we can order through all the numbers with the property $\mathcal{P} + 1$ if we have already ordered all the numbers with the property $\mathcal{P}$.

Armed with ordinal knowledge, we are now ready to tackle the ordinal proofs.

3. Gentzen's consistency proof with ε_0

3.1. **Brief historical background: Hilbert's second problem, Gödel's second incompleteness theorem, and Gentzen's motivations.** In 1900, Hilbert put forward his second problem, asking for a proof that arithmetic is consistent, or in other words, free of internal contradictions. In mathematical terms, for any formal arithmetic system $\mathbf{F}$, we can create some formula $Cons(\mathbf{F})$ that describes the consistency of $\mathbf{F}$ by encoding in it the property that no natural number codes for the contradictory equation $0 = 1$. In 1931, Kurt Gödel published his second incompleteness theorem that proved that any system of mathematics, no matter how elementary (such as Peano arithmetic was designed to be), could not prove its own consistency: $Cons(\mathbf{F})$ cannot be proven under $\mathbf{F}$.

Effectively, this meant that the proof for the consistency of a mathematical system had to come from a different system, the consistency of which would also be in question. In an effort to provide a positive solution to Hilbert's second problem, Gerhard Gentzen published a paper in 1936 [Gen36] showing how Peano arithmetic does not contain contradictions (i.e. it is consistent), provided that another system, **primitive recursive arithmetic** (PRA for short, and similar to Peano arithmetic but a more bare-bones system without many controversial axioms regarding inference) bundled with acceptance of transfinite induction up to ε_0, does not contain contradictions (i.e. it is also consistent).

3.2. **Preliminaries to Gentzen's theorem.** Gentzen's theorem and his proof proceeds in three parts:

(1) Any value of truth for the consistency of any "derivation" (a sequence of steps in a proof) is "reduced" to the values of truth for the consistencies of simpler derivations that led to the previous derivation. What exactly we mean by "derivation" will be explained below.

(2) A transfinite ordinal number (an ordinal less than ε_0) is associated with every derivation and for each reduction. Inconsistency is coded into a derivation and we find a contradiction if we assume there to be an inconsistency in Peano arithmetic.
(3) All derivation consistencies follow from transfinite induction.

3.3. **Notations and definitions.** Gentzen's proof relies on a system known as LK-calculus that will be explained and formalized as follows. It is not of the uppermost necessity to understand all the notation, the fundamental ideas are more important.

(1) The only numeral is 1, all numbers are greater than or equal to 1.
(2) Functions are not used in this system except for one, the successor function $S(x)$, where the successor of 1 (which is 2 in our system) is denoted $S(1)$. For shorthand, it will also be denoted $1'$.
(3) The only logic symbols used are $\wedge$ (logical AND, conjunction), $\neg$ (logical NOT, negation), $\vee$ (logical OR, disjunction), $\exists$ (there exists), and $\forall$ (for all). The first three are called *logical connectives*.
(4) A *formula* is a set of arbitrary terms (like 1, $1''$, and α) connected with these logical symbols. These are denoted with calligraphic letters below, such as $\mathcal{A}$, and a sequence of various formulae is denoted with blackboard letters, such as $\mathbb{P}$.
(5) *Prime formulas* do not contain logical connectives, only $=$ signs.
(6) The *terminal connective* of a non-prime formula is the logical connective added last in the formula's construction. For example, the terminal connective of $\forall x(x > 1')$ is $\forall$.
(7) The *degree* of a formula is the total number of logical connectives the formula has.
(8) A *sequent* is an expression of the form $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_m \implies \mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_n$ for some natural numbers m, n. All the $\mathcal{A}$'s are known as the *antecedent formulae* and all the $\mathcal{B}$'s are known as the *succedent formulae*. Any antecedent and any succedent can be empty, and each formula's truth value is known.
(9) Any sequent is false if all antecedent formulae are true and all succedent formulae are false. If at least one succedent formula is true, then the entire sequent is considered true regardless. In other words, $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_m \implies \mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_n$ can be read as "If the assumptions $\mathcal{A}$ are true, then at least one of the propositions $\mathcal{B}$ holds".
(10) An *inference figure* involves an *upper sequent*, a *lower sequent*, and a *line of inference* written between them. This can be read as "Given the statement of the upper sequent is true, we can infer the lower sequent to be true as well". For example, $\frac{\mathcal{A},\mathcal{B} \implies \mathcal{C}}{\mathcal{A},\mathcal{B} \implies 1=1}$ can be read as "Given $\mathcal{A}$ and $\mathcal{B}$ imply $\mathcal{C}$, we can infer $\mathcal{A}$ and $\mathcal{B}$ to imply that $1 = 1$". Of course, what this actually means depends on what $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are.
(11) The *structural inference figures* describe four different valid manipulations of sequents, that preserve truth values for the upper and lower sequents.

Definition 3.1. A *thinning* is defined as an action that adds extra antecedents and succedents to the upper sequent to obtain the lower sequent. $\frac{\mathbb{P} \implies \mathbb{Q}}{\mathcal{A},\mathbb{P} \implies \mathbb{Q}}$ can be read as "If $\mathbb{P}$ implies $\mathbb{Q}$, then a different condition $\mathcal{A}$ and $\mathbb{P}$ also implies $\mathbb{Q}$." $\frac{\mathbb{P} \implies \mathbb{Q}}{\mathbb{P} \implies \mathbb{Q},\mathcal{A}}$ can be read as "If $\mathbb{P}$ implies $\mathbb{Q}$, then $\mathbb{P}$ also implies at least one of $\mathbb{Q}$ and $\mathcal{A}$."

Definition 3.2. A *contraction* is defined as an action that removes duplicate antecedents and succedents from the upper sequent to obtain the lower sequent. $\frac{\mathcal{A},\mathcal{A},\mathbb{P} \implies \mathbb{Q}}{\mathcal{A},\mathbb{P} \implies \mathbb{Q}}$

can be read as "If $\mathcal{A}$, $\mathcal{A}$, and $\mathbb{P}$ imply $\mathbb{Q}$, then $\mathcal{A}$ and $\mathbb{P}$ imply $\mathbb{Q}$." $\frac{\mathbb{P} \implies \mathbb{Q},\mathcal{A},\mathcal{A}}{\mathbb{P} \implies \mathbb{Q},\mathcal{A}}$ can be read as "If $\mathbb{P}$ implies $\mathbb{Q}$, $\mathcal{A}$, and $\mathcal{A}$, then $\mathbb{P}$ implies $\mathbb{Q}$ and $\mathcal{A}$."

Definition 3.3. An *interchange* is defined as an action that changes the order of antecedents and succedents from the upper sequent to obtain the lower sequent. $\frac{\mathbb{O},\mathcal{A},\mathcal{B},\mathbb{P}, \implies \mathbb{Q}}{\mathbb{O},\mathcal{B},\mathcal{A},\mathbb{P} \implies \mathbb{Q}}$ can be read as "If $\mathbb{O}$, $\mathcal{A}$, $\mathcal{B}$, and $\mathbb{P}$ imply $\mathbb{Q}$, then $\mathbb{O}$, $\mathcal{B}$, $\mathcal{A}$, and $\mathbb{P}$ imply $\mathbb{Q}$." $\frac{\mathbb{P} \implies \mathbb{Q},\mathcal{A},\mathcal{B},\mathbb{R}}{\mathbb{P} \implies \mathbb{Q},\mathcal{B},\mathcal{A},\mathbb{R}}$ can be read as "If $\mathbb{P}$ implies $\mathbb{Q}$, $\mathcal{A}$, $\mathcal{B}$, and $\mathbb{R}$, then $\mathbb{P}$ implies $\mathbb{Q}$, $\mathcal{B}$, $\mathcal{A}$, and $\mathbb{R}$."

Definition 3.4. A *cut* is defined as an action that combines the respective antecedents and succedents of two upper sequents to obtain the lower sequent. $\frac{\mathbb{P} \implies \mathbb{Q},\mathcal{A} \quad \mathcal{A},\mathbb{O} \implies \mathbb{R}}{\mathbb{P},\mathbb{O} \implies \mathbb{Q},\mathbb{R}}$ can be read as "If $\mathbb{P}$ implies $\mathbb{Q}$ and $\mathcal{A}$, and $\mathcal{A}$ and $\mathbb{O}$ imply $\mathbb{R}$, then $\mathbb{P}$ and $\mathbb{O}$ imply $\mathbb{Q}$ and $\mathbb{R}$.".

(12) The *operational inference figures* in Figure 7 demonstrate how the five different logical symbols $(\wedge, \vee, \forall, \exists, \neg)$ are encoded in the inference figures.

$$\wedge\text{:}\ \frac{\mathbb{P} \implies \mathbb{Q},\mathcal{A} \quad \mathbb{P} \implies \mathbb{Q},\mathcal{B}}{\mathbb{P} \implies \mathbb{Q},\mathcal{A}\wedge\mathcal{B}} \text{ and } \frac{\mathcal{A},\mathbb{P} \implies \mathbb{Q}}{\mathcal{A}\wedge\mathcal{B},\mathbb{P} \implies \mathbb{Q}} \text{ and } \frac{\mathcal{B},\mathbb{P} \implies \mathbb{Q}}{\mathcal{A}\wedge\mathcal{B},\mathbb{P} \implies \mathbb{Q}}$$

$$\vee\text{:}\ \frac{\mathcal{A},\mathbb{P} \implies \mathbb{Q} \quad \mathcal{B},\mathbb{P} \implies \mathbb{Q}}{\mathcal{A}\vee\mathcal{B},\mathbb{P} \implies \mathbb{Q}} \text{ and } \frac{\mathbb{P} \implies \mathbb{Q},\mathcal{A}}{\mathbb{P} \implies \mathbb{Q},\mathcal{A}\vee\mathcal{B}} \text{ and } \frac{\mathbb{P} \implies \mathbb{Q},\mathcal{B}}{\mathbb{P} \implies \mathbb{Q},\mathcal{A}\vee\mathcal{B}}$$

$$\forall\text{:}\ \frac{\mathbb{P} \implies \mathbb{Q},\mathcal{F}(a)}{\mathbb{P} \implies \mathbb{Q},\forall_x\mathcal{F}(x)} \text{ and } \frac{\mathcal{F}(a),\mathbb{P} \implies \mathbb{Q}}{\forall_x\mathcal{F}(x),\mathbb{P} \implies \mathbb{Q}}$$

$$\exists\text{:}\ \frac{\mathcal{F}(a),\mathbb{P} \implies \mathbb{Q}}{\forall_x\mathcal{F}(x),\mathbb{P} \implies \mathbb{Q}} \text{ and } \frac{\mathbb{P} \implies \mathbb{Q},\mathcal{F}(a)}{\mathbb{P} \implies \mathbb{Q},\exists_x\mathcal{F}(x)}$$

$$\neg\text{:}\ \frac{\mathcal{A},\mathbb{P} \implies \mathbb{Q}}{\mathbb{P} \implies \mathbb{Q},\neg\mathcal{A}} \text{ and } \frac{\mathbb{P} \implies \mathbb{Q},\mathcal{A}}{\neg\mathcal{A},\mathbb{P} \implies \mathbb{Q}}$$

Figure 7. Five different logic symbols, with usage demonstrated in operational inference structures. View each inference figure as separate from any others.

(13) *CJ-inference figures* are unlike structural and operational inference figures, specifically used to encode induction. These follow the format

$$\frac{\mathcal{F}(a) \implies \mathcal{F}(a)'}{\mathcal{F}(1) \implies \mathcal{F}(t)},$$

where a is a free variable and t ranges from 1 up to a. The logical reasoning behind the above format should be very clear. The upper sequent describes the second step of induction: something is true for a certain a implies it is true for $a + 1$, or the successor of a. The lower sequent describes the third step, where we can go from 1 (which is true because we put it in the antecedent) up to as high as we want, perhaps up to a certain t.

(14) A *derivation* is a tree-like figure with basic sequents found at the top branches and a lowest sequent, the *endsequent*, found at the root of the tree. The relationship between connected branches is described using inference figures. An example of a possible derivation is given by Figure 8.

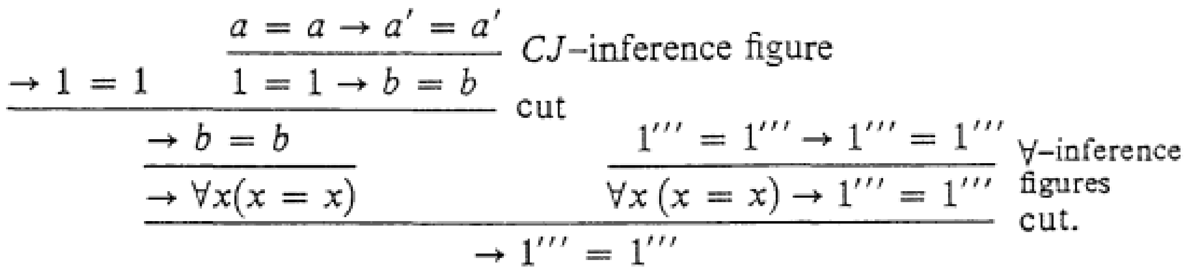

Figure 8. An example of a derivation. Picture from *The Collected Papers of Gerhard Gentzen.*

In this system, lacking antecedent formulae before $\Longrightarrow$ signifies that the succedent formulae are true, regardless of initial assumptions. On the other hand, lacking succedent formulae after $\Longrightarrow$ signifies that the assumptions made in the antecedent formulae create a contradiction as you can't make any formulae. Thus, an empty sequent, one with no antecedent or succedent formulae, demonstrates that without any prior assumptions, a contradiction will result in a system. The way we prove the consistency of Peano arithmetic is by proving that an empty sequent *cannot* be found or deduced through a derivation in this system.

3.4. **Outline of Gentzen's proof.** Due to its dense mathematical notation and its sheer length, the proof will be explained conceptually below. Readers are recommended to read Sections 4 and 8 of Gerhard Gentzen's papers on the proof [Kre71].

The first step to proving an empty sequent can't be found or deduced in a system is to create a methodical system that can reduce all logical connectives to simpler statements that can create an empty sequent.

Suppose a derivation exists that leads to an endsequent that is the empty sequent. We can change the manner of this derivation into a simpler derivation that will still have the same endsequent, using the rules that we have stated above. The justification for this is easy to see if we presume there is a step in the derivation somewhere with the most complexity out of all of the steps. It must be reducible in some form, because the only way it could enter the derivation would be if it was introduced somewhere and then cut-out and eliminated elsewhere such that the endsequent would be empty and thus the empty sequent.

The manner in which we can reduce steps is done via Figure 9. Due to the size of the inference figure if written out completely, the derivation tree is written with each inference figure as a number, to be replaced with an inference figure from Table 2. The reader

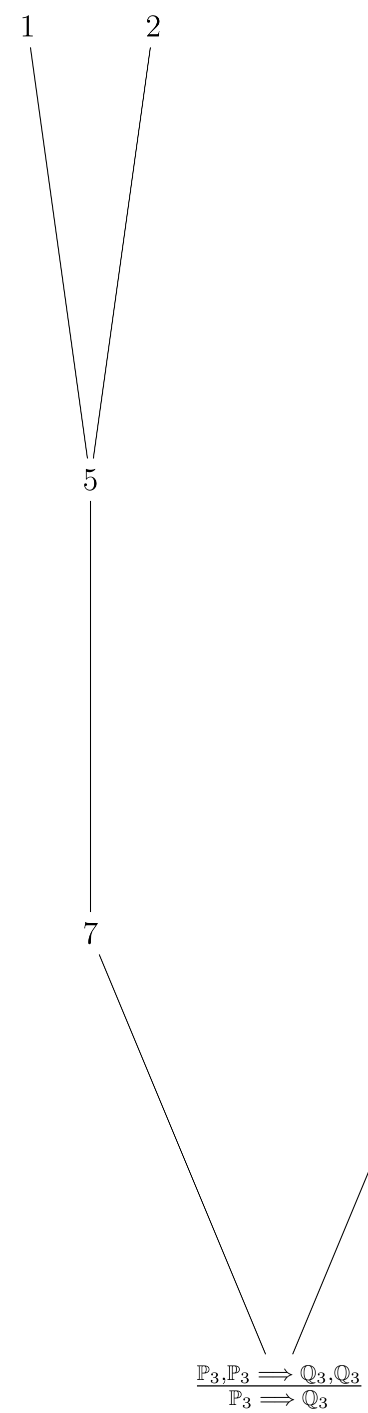

Figure 9. The reduction steps for all terminal connectives involves changing the derivation into the above format.

can verify that substituting all the values of the table into the tree will lead to an accurate reduction step for all five logical symbols noted above.

The inference figures positioned at numbers 1 and 2 are made to describe general statements for each general logical symbol in the system, before being reduced using the structural

Tree Position	$\forall$	$\wedge$
1	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{F}(n)}{\mathbb{P}_1 \Longrightarrow \mathcal{F}(n),\mathbb{Q}_1,\forall_x\mathcal{F}(x)}$	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A} \quad \mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{B}}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\, \mathcal{A}\wedge\mathcal{B}}$
2	$\frac{\mathcal{F}(n),\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\forall_x\mathcal{F}(x),\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$	$\frac{\mathcal{A},\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\mathcal{A}\wedge\mathcal{B},\, \mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$
3	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{F}(a)}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\forall_x\mathcal{F}(x)}$	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A}}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A}\wedge\mathcal{B}}$ or $\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{B}}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A}\wedge\mathcal{B}}$
4	$\frac{\mathcal{F}(n),\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\forall_x\mathcal{F}(x),\mathbb{P}_2,\mathcal{F}(n) \Longrightarrow \mathbb{Q}_2}$	$\frac{\mathcal{B},\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\mathcal{A}\wedge\mathcal{B},\, \mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$ or $\frac{\mathcal{A},\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\mathcal{A}\wedge\mathcal{B},\, \mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$
5	$\frac{\mathbb{P} \Longrightarrow \mathcal{F}(n),\mathbb{Q},\forall_x\mathcal{F}(x) \quad \forall_x\mathcal{F}(x),\mathbb{O} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O} \Longrightarrow \mathcal{F}(n),\mathbb{Q},\mathbb{R}}$	$\frac{\mathbb{P} \Longrightarrow \mathcal{A},\mathbb{Q},\mathcal{A}\wedge\mathcal{B} \quad \mathcal{A}\wedge\mathcal{B},\mathbb{O} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O} \Longrightarrow \mathcal{A},\mathbb{Q},\mathbb{R}}$ or $\frac{\mathbb{P} \Longrightarrow \mathcal{B},\mathbb{Q},\mathcal{A}\wedge\mathcal{B} \quad \mathcal{A}\wedge\mathcal{B},\mathbb{O} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O} \Longrightarrow \mathcal{B},\mathbb{Q},\mathbb{R}}$
6	$\frac{\mathbb{P} \Longrightarrow \mathbb{Q},\forall_x\mathcal{F}(x) \quad \forall_x\mathcal{F}(x),\mathbb{O},\mathcal{F}(n) \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O},\mathcal{F}(n) \Longrightarrow \mathbb{Q},\mathbb{R}}$	$\frac{\mathbb{P} \Longrightarrow \mathbb{Q},\mathcal{A}\wedge\mathcal{B} \quad \mathcal{A}\wedge\mathcal{B},\mathbb{O},\mathcal{B} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O},\mathcal{B} \Longrightarrow \mathbb{Q},\mathbb{R}}$ or $\frac{\mathbb{P} \Longrightarrow \mathbb{Q},\mathcal{A}\wedge\mathcal{B} \quad \mathcal{A}\wedge\mathcal{B},\mathbb{O},\mathcal{A} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O},\mathcal{A} \Longrightarrow \mathbb{Q},\mathbb{R}}$
7	$\frac{\mathbb{P}_3 \Longrightarrow \mathcal{F}(n),\mathbb{Q}_3}{\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3,\mathcal{F}(n)}$	$\frac{\mathbb{P}_3 \Longrightarrow \mathcal{A},\mathbb{Q}_3}{\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3,\mathcal{A}}$ or $\frac{\mathbb{P}_3 \Longrightarrow \mathcal{B},\mathbb{Q}_3}{\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3,\mathcal{B}}$
8	$\frac{\mathbb{P}_3,\mathcal{F}(n) \Longrightarrow \mathbb{Q}_3}{\mathcal{F}(n),\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3}$	$\frac{\mathbb{P}_3,\mathcal{B} \Longrightarrow \mathbb{Q}_3}{\mathcal{B},\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3}$ or $\frac{\mathbb{P}_3,\mathcal{A} \Longrightarrow \mathbb{Q}_3}{\mathcal{A},\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3}$

Tree Position	$\exists$	$\vee$
1	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{F}(n)}{\mathbb{P}_1 \Longrightarrow \mathcal{F}(n),\mathbb{Q}_1,\exists_x\mathcal{F}(x)}$	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A} \quad \mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{B}}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\, \mathcal{A}\vee\mathcal{B}}$
2	$\frac{\mathcal{F}(n),\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\exists_x\mathcal{F}(x),\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$	$\frac{\mathcal{A},\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\mathcal{A}\vee\mathcal{B},\, \mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$
3	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{F}(a)}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\exists_x\mathcal{F}(x)}$	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A}}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A}\vee\mathcal{B}}$ or $\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{B}}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A}\vee\mathcal{B}}$
4	$\frac{\mathcal{F}(n),\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\exists_x\mathcal{F}(x),\mathbb{P}_2,\mathcal{F}(n) \Longrightarrow \mathbb{Q}_2}$	$\frac{\mathcal{B},\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\mathcal{A}\vee\mathcal{B},\, \mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$ or $\frac{\mathcal{A},\mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}{\mathcal{A}\vee\mathcal{B},\, \mathbb{P}_2 \Longrightarrow \mathbb{Q}_2}$
5	$\frac{\mathbb{P} \Longrightarrow \mathcal{F}(n),\mathbb{Q},\exists_x\mathcal{F}(x) \quad \exists_x\mathcal{F}(x),\mathbb{O} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O} \Longrightarrow \mathcal{F}(n),\mathbb{Q},\mathbb{R}}$	$\frac{\mathbb{P} \Longrightarrow \mathcal{A},\mathbb{Q},\mathcal{A}\vee\mathcal{B} \quad \mathcal{A}\vee\mathcal{B},\mathbb{O} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O} \Longrightarrow \mathcal{A},\mathbb{Q},\mathbb{R}}$ or $\frac{\mathbb{P} \Longrightarrow \mathcal{B},\mathbb{Q},\mathcal{A}\vee\mathcal{B} \quad \mathcal{A}\vee\mathcal{B},\mathbb{O} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O} \Longrightarrow \mathcal{B},\mathbb{Q},\mathbb{R}}$
6	$\frac{\mathbb{P} \Longrightarrow \mathbb{Q},\exists_x\mathcal{F}(x) \quad \exists_x\mathcal{F}(x),\mathbb{O},\mathcal{F}(n) \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O},\mathcal{F}(n) \Longrightarrow \mathbb{Q},\mathbb{R}}$	$\frac{\mathbb{P} \Longrightarrow \mathbb{Q},\mathcal{A}\vee\mathcal{B} \quad \mathcal{A}\vee\mathcal{B},\mathbb{O},\mathcal{B} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O},\mathcal{B} \Longrightarrow \mathbb{Q},\mathbb{R}}$ or $\frac{\mathbb{P} \Longrightarrow \mathbb{Q},\mathcal{A}\vee\mathcal{B} \quad \mathcal{A}\vee\mathcal{B},\mathbb{O},\mathcal{A} \Longrightarrow \mathbb{R}}{\mathbb{P},\mathbb{O},\mathcal{A} \Longrightarrow \mathbb{Q},\mathbb{R}}$
7	$\frac{\mathbb{P}_3 \Longrightarrow \mathcal{F}(n),\mathbb{Q}_3}{\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3,\mathcal{F}(n)}$	$\frac{\mathbb{P}_3 \Longrightarrow \mathcal{A},\mathbb{Q}_3}{\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3,\mathcal{A}}$ or $\frac{\mathbb{P}_3 \Longrightarrow \mathcal{B},\mathbb{Q}_3}{\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3,\mathcal{B}}$
8	$\frac{\mathbb{P}_3,\mathcal{F}(n) \Longrightarrow \mathbb{Q}_3}{\mathcal{F}(n),\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3}$	$\frac{\mathbb{P}_3,\mathcal{B} \Longrightarrow \mathbb{Q}_3}{\mathcal{B},\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3}$ or $\frac{\mathbb{P}_3,\mathcal{A} \Longrightarrow \mathbb{Q}_3}{\mathcal{A},\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3}$

Tree Position	$\neg$
1	–
2	–
3	$\frac{\mathcal{A},\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1}{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\neg\mathcal{A}}$
4	$\frac{\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,\mathcal{A}}{\neg\mathcal{A},\mathbb{P}_1 \Longrightarrow \mathbb{Q}_1,}$
5	–
6	–
7	–
8	$\frac{\mathbb{P}_3,\mathcal{A} \Longrightarrow \mathbb{Q}_3}{\mathcal{A},\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3}$

Table 2. The reduction step for the five terminal connectives involves changing the derivation using the above table. The symbol $\neg$ requires only the right side of the tree.

inference figures to reach the final step of $\mathbb{P}_3 \Longrightarrow \mathbb{Q}_3$. We will assume that there exists some sequence of derivations that turn this final lower sequent into the empty sequent.

Thus, we have so far demonstrated that for any simple sequent that involves the five logical symbols of $\forall$, $\wedge$, $\exists$, $\vee$, and $\neg$, we can define a reduction step that reduces all such sequents to a simple "The formulae $\mathbb{P}_3$ imply the formulae $\mathbb{Q}_3$." The next step involves ordinal association with each step.

Suppose we have an arbitrary derivation. The ordinal number correlated with this derivation is calculated by going down from the uppermost sequents and giving each sequent an ordinal number. We start by giving the uppermost sequents of the entire tree the ordinal number 1 (or ω^0).

Now, we deduce the ordinal for the line of inference. For every structural inference figure, the ordinal number for the upper sequent of an inference figure remains unchanged, unless it is a cut, in which case we take the natural sum of the ordinal numbers of the upper two sequents. If the inference figure is operational (following Table 2), then +1 is added to the ordinal number of the upper sequent, unless there are two upper sequents, in which case the larger of the two ordinal numbers is selected and +1 is added to it. Finally, if we have a CJ-inference figure with an upper sequent ordinal of the form $\omega^{\alpha_n} + \cdots \omega^{\alpha_1}$, then the ordinal for the line of inference of the CJ-inference figure is assigned to be ω^{α_n+1}.

Finally, we deduce the ordinal for the lower sequent. Let the ordinal of the line of reference be λ. If the level (number of logical connectives and quantifiers) of the lower sequent is the same or less than that of the upper sequent, then the ordinal number of the lower sequent is equal to the ordinal number of the higher sequent. If its level is lower by 1, then the ordinal number of the lower sequent is ω^λ. If it is lower by two, then the ordinal number of the lower sequent is ω^{ω^λ}, if lower by three, then it is $\omega^{\omega^{\omega^\lambda}}$, etc. The ordinal number obtained for the endsequent of the derivation is the ordinal number for the entire derivation.

Table 3 provides a handy chart for reference. As an example, let us assign ordinals to the derivation tree for Figure 8. The highest sequent, $a = a \implies a' = a'$ is assigned an order type of 1 (or ω^0). The order type of the line of inference directly below is ω^{0+1}, or ω, and the order type of the lower sequent of the CJ-inference figure, $1 = 1 \implies b = b$, is also 1, because it has the same level as the upper sequent. Paired with the upper sequent $\implies 1 = 1$ for a cut, the upper sequents together have a natural sum of 2, assigned to the cut's line of inference. The overall level of both upper sequents is 0, and so the lower sequent $\implies b = b$ also has an ordinal of the upper sequent's natural sum: 2. The line of inference afterwards is part of an operational inference figure, so the ordinal is 2 incremented by 1, or 3. The lower sequent of the $\forall$-operational inference figure, $\forall x(x = x)$, has level 1 as opposed to the upper sequent, so the ordinal remains at 3.

Now, we shift to the other side, with $1''' = 1''' \implies 1''' = 1'''$, with an order type of 1. The line of inference, likewise, increments by 1, to achieve 2. The resulting right-hand lower sequent, $\forall x(x = x) \implies 1''' = 1'''$, has level 1, higher than the level of the one above it, so the ordinal assigned to it is also 2.

Now that the two sides of the tree have come together, the line of inference is assigned an ordinal of $2 + 2 = 4$, and the lower sequent, $\implies 1''' = 1'''$, having two less $\forall$'s than the upper sequents, is assigned an ordinal ω^{ω^4}, which is also the ordinal assigned to the entire derivation. Notice that through this entire process, there is no opportunity for the ordinal assigned to each sequent or inference figure to decrease at all.

Condition	**Line of inference's order**
Structural inference figure	$\eta(S_{upper})$
Structural inference figure with cut	$\eta(S_{upper_1}) \# \eta(S_{upper_2})$
Operational inference figure	$\eta(S_{upper}) + 1$
Operational inference figure with two sequents	$max(\eta(S_{upper_1}), \eta(S_{upper_2})) + 1$
CJ-inference figure	$\omega^{\alpha_{max}+1}$

Condition	**Lower sequent's order**
$\phi(S_{lower}) \geq \phi(S_{upper})$	$\eta(L)$
$\phi(S_{lower}) = \phi(S_{upper}) - 1$	$\omega^{\eta(L)}$
$\phi(S_{lower}) = \phi(S_{upper}) - 2$	$\omega^{\omega^{\eta(L)}}$
$\phi(S_{lower}) = \phi(S_{upper}) - 3$	$\omega^{\omega^{\omega^{\eta(L)}}}$
$\phi(S_{lower}) = \phi(S_{upper}) - n$	$\omega^{\omega^{\cdots\eta(L)}}$, for n ω's

Table 3. Let $\eta(S)$ be the ordinal corresponding to a certain sequent S, and let $\eta(L)$ be the ordinal that corresponds to a certain line of inference L. α_{max} represents the largest ordinal power of η, and $\phi(S)$ represents the level (number of logical connectives and quantifiers) of a certain sequent S.

We shall now prove that ordinal numbers will in fact decrease through the course of a reduction step on the way to the empty sequent.

Suppose that the ordinal corresponding to a certain sequent S is denoted $\eta(S)$, and we have the upper sequent represented as S_{upper} and the lower sequent represented as S_{lower}. The upper sequent of a CJ-inference figure is $\eta(S_{upper})$, and thus the line of inference would have the ordinal $\omega^{\alpha_{max}+1}$, which is also the ordinal number for the lower sequent, which cannot be lower than that of the upper sequent because of the way we have defined the assignment of ordinals. Now, if we look at the reduced form of the CJ-inference figure, each one of its uppermost sequents receives the same ordinal number $\eta(S_{upper})$. Because all sequents of the replacement figure must have the same level as the two sequents of the CJ-inference figure from before, the ordinal number assigned to this lowest sequent of the figure is therefore equal to the natural sum of all the numbers at the very beginning of the CJ-inference figure, $\eta(S_{upper})$. Because $\eta(S_{upper})$ is of the form $\omega^{\alpha_{max}} + \cdots \omega^{\alpha_{min}}$, it is therefore less than $\omega^{\alpha_{max}+1}$ according to the manner in which ordinal size comparison is defined (remember, it is non-commutative). Therefore, we have shown that the ordinals have somehow decreased going down the derivation.

Gentzen goes on to create a specific reduction formula (a special kind of cut-elimination) for each of the logical connectives and shows how each one can be used with a CJ-inference figure to decrease the size of the ordinal. In the set of all possible derivational trees in this mathematical system, Gentzen shows that this workable formula leads to an infinitely and strictly descending sequence of ordinals all less than ε_0 corresponding to a recursively-acting formula on all possible sequents if one tries to reduce these sequents to the empty sequent. The method in which he shows this is not important, but it is important to see why an infinitely descending sequence of ordinals is not possible.

Let us instead presume that an infinite descending sequence of ordinals, all less than ε_0, is in fact possible. Let's include all the ordinals in this descending sequence in the set O.

All sets of ordinals are defined to well-ordered, as shown way back in 2.5, and the definition necessarily entails that the set contains a least element, so O must have a least element. However, if we try to define a minimum element of O, such as O_{min}, we can always find a lesser element farther down the sequence. Therefore, that means O itself cannot exist.

Since an infinitely descending sequence of ordinals cannot exist, then that means we are unable to construct an empty sequent. If we are unable to construct an empty sequent in this system of LK-calculus, it is impossible for the system of elementary Peano arithmetic to have an inconsistency, which means Peano arithmetic must, in fact, be consistent.

3.5. **Analysis of Gentzen's results.** While Peano arithmetic could not prove Peano arithmetic's consistency, ordinal arithmetic could, though the extent of its success is debatable. While PRA was viewed to be less controversially consistent due to it being quantifier-free (lacking $\forall$ and $\exists$) and finitistic (not including an axiom with the idea of infinity), Gentzen had to extend it to include transfinite induction, which may or may not be considered finitistic due to the introduction of the ordinal ε_0.

While there are many solutions to Hilbert's second problem in other mathematical systems, such as Zermelo-Fraenkel set theory, some mathematicians do not accept these "higher-strength" mathematical systems, given Peano arithmetic itself is in doubt. Therefore, a full solution Hilbert's second problem would have to contain only principles that are viewed as so fundamental and obvious that they would be acceptable to those who doubt the consistency of Peano arithmetic in the first place.

For any two formal systems **A** and **B**, **B** can be considered *stronger* than **A** if **B** can prove a wider range of mathematical statements compared to **A**. The PRA and ε_0 system that Gentzen used turns out to be incomparable with Peano arithmetic, as there are some things that Gentzen's system can prove that Peano arithmetic can't (the consistency of Peano arithmetic) and there are some things that Peano arithmetic can prove that Gentzen's system can't (ordinary mathematical induction, which is strictly contained in the axioms of Peano arithmetic).

So what about the PRA and ε_0 system is still inadequate for decidedly proving Peano arithmetic's consistency? It turns out that Gentzen also proved that transfinite induction up to ε_0 under Peano arithmetic is itself unprovable under Peano arithmetic. The proof of this non-provability would be excessively tedious to explain, but a further explanation and the full proof can be found in Gentzen's collected papers, which are included in this paper's references.

A brief and indirect justification for the non-provability of transfinite induction comes in the form of Gödel's incompleteness theorem. If transfinite induction could be proved with Peano arithmetic, then Peano arithmetic would thus prove a different system and then succeed in proving its own consistency, which would create a contradiction.

To this day, Hilbert's second problem is an open question, and there is still no widespread consensus regarding whether or it not it was ever "solved".

4. Goodstein's Theorem

4.1. **Introduction.** Goodstein's theorem, as opposed to the formal and sometimes tedious set logic rigor of Gentzen's consistency proof, is a statement about a very simple set of rules that leads to a sequence of numbers that grow absurdly quickly, yet has a very interesting final property.

Theorem 4.1 (Goodstein's Theorem)**.** *Every Goodstein sequence eventually terminates at 0.*

It was proved in 1944 by Reuben Goodstein [Goo44] using ordinal arithmetic, and shockingly, it turns out that it is impossible to prove it with Peano arithmetic.

4.2. **Hereditary base-n notation.** Firstly, to explain the theorem and Goodstein sequences, we must have an introduction as to what is known as hereditary base-n notation.

For all natural numbers $b > 1$, any natural number n can be expressed as $c_k b^k + \cdots + c_2 b^2 + c_1 b^1 + c_0 b^0$, for any c_i where $0 \leq c_i < b$ and b^i for $0 \leq i \leq k$. As an example, take $n = 123$ and $b = 2$:

$$n = 123 = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

It is easy to notice that this is equivalent to representing n in a certain base-b. This is standard base-notation.

To achieve hereditary base notation, all exponents are written in base-notation as well. Then, the resulting exponents of the exponents are also written in base-notation. We repeat until all numbers are written in base-b. Returning to our $n = 123$ example, we can write it as such:

$$n = 123 = 1 \cdot 2^{2^2+2^1} + 1 \cdot 2^{2^2+1} + 1 \cdot 2^{2^2} + 1 \cdot 2^{2^1+1} + 1 \cdot 2^1 + 1.$$

We usually write replace all b^0's with 1 as it makes it easier to read.

4.3. **Goodstein Sequences.**

Definition 4.2. A *Goodstein sequence* is defined sequentially as follows. Let the first element of a Goodstein sequence of a certain n, $G(n)$, be n itself. Let us denote this first element $G(n)_1$. The second element $G(n)_2$ is generated by writing $G(n)_1$ in hereditary base-2 notation, changing all 2's to 3's, and subtracting 1. In general, any kth element $G(n)_k$ can be found by writing $G(n)_{k-1}$ in hereditary base-k notation, changing all k's to $k+1$'s, and finally subtracting 1. The sequence terminates after the first element in the sequence that is 0.

For example, the Goodstein sequence for 123, $G(123)$ has the following entries:

Index	$G(123)$
1	123
2	$123 = 1 \cdot 2^{2^2+2^1} + 1 \cdot 2^{2^2+1} + 1 \cdot 2^{2^2} + 1 \cdot 2^{2^1+1} + 1 \cdot 2^1 + 1$
	$\downarrow$
	$(1 \cdot 3^{3^3+3^1} + 1 \cdot 3^{3^3+1} + 1 \cdot 3^{3^3} + 1 \cdot 3^{3^1+1} + 1 \cdot 3^1 + 1) - 1 = 236393522034681$
3	$236393522034681 = 1 \cdot 3^{3^3+3^1} + 1 \cdot 3^{3^3+1} + 1 \cdot 3^{3^3} + 1 \cdot 3^{3^1+1} + 1 \cdot 3^1$
	$\downarrow$
	$(1 \cdot 4^{4^4+4^1} + 1 \cdot 4^{4^4+1} + 1 \cdot 4^{4^4} + 1 \cdot 4^{4^1+1} + 1 \cdot 4^1) - 1 \approx 3.499 \times 10^1 56$
...	...

Table 4. The Goodstein sequence for 123.

Since the numbers we notice from this sequence are truly astronomical, it may prove to be more useful to first analyze the behaviors of smaller numbers.

Index	$G(2)$
1	$\mathbf{2}$
2	$2 = 1 \cdot 2^1$ $\downarrow$ $(1 \cdot 3^1) - 1 = \mathbf{2}$
3	$2 = 2 \cdot 3^0$ $\downarrow$ $(2 \cdot 4^0) - 1 = \mathbf{1}$
4	$1 = 1 \cdot 4^0$ $\downarrow$ $(1 \cdot 5^0) - 1 = \mathbf{0}$

Table 5. The Goodstein sequence for 2. All b^0's are written out for clarity.

Index	$G(3)$
1	$\mathbf{3}$
2	$3 = 1 \cdot 2^1 + 1 \cdot 2^0$ $\downarrow$ $(1 \cdot 3^1 + 1 \cdot 3^0) - 1 = \mathbf{3}$
3	$3 = 1 \cdot 3^1$ $\downarrow$ $(1 \cdot 4^1) - 1 = \mathbf{3}$
4	$3 = 3 \cdot 4^0$ $\downarrow$ $(3 \cdot 5^0) - 1 = \mathbf{2}$
5	$2 = 2 \cdot 5^0$ $\downarrow$ $(2 \cdot 6^0) - 1 = \mathbf{1}$
6	$1 = 1 \cdot 6^0$ $\downarrow$ $(1 \cdot 7^0) - 1 = \mathbf{0}$

Table 6. The Goodstein sequence for 3. All b^0's are written out for clarity.

And of course, $G(0)$ will be an infinite sequence of 0's and $G(1)$ will have a first element 1 and then continue onward with an infinite sequence of 0's.

While there are several interesting features about these sequences upon first glance that may help in our proof of the sequences' eventual termination, such as how any sequence reaches its highest point and then how every subsequent number slowly decreases by 1, the actual proof that all sequences terminate is in fact more abstract.

4.4. **Ordinal proof of Goodstein's Theorem.**

Proof. Suppose that for a Goodstein sequence $G(n)$ of a certain number n, there is a bijective sequence $O(n)$ of ordinals that is strictly decreasing. Notice that unlike in Gentzen's proof, $O(n)$, while descending in nature, is not infinite, so it does not break our requirements that the set has a least element. The bijection between the two sequences ensures that

Index	$G(4)$
1	**4**
2	$4 = 1 \cdot 2^{2^1}$ $\downarrow$ $(1 \cdot 3^{3^1}) - 1 = \mathbf{26}$
3	$26 = 2 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0$ $\downarrow$ $(2 \cdot 4^2 + 2 \cdot 4^1 + 2 \cdot 4^0) - 1 = \mathbf{41}$
4	$41 = 2 \cdot 4^2 + 2 \cdot 4^1 + 1 \cdot 4^0$ $\downarrow$ $(2 \cdot 5^2 + 2 \cdot 5^1 + 1 \cdot 5^0) - 1 = \mathbf{60}$
5	$60 = 2 \cdot 5^2 + 2 \cdot 5^1$ $\downarrow$ $(2 \cdot 6^2 + 2 \cdot 6^1) - 1 = \mathbf{83}$
6	$83 = 2 \cdot 6^2 + 1 \cdot 6^1 + 5 \cdot 6^0$ $\downarrow$ $(2 \cdot 7^2 + 1 \cdot 7^1 + 5 \cdot 7^0) - 1 = \mathbf{109}$
7	$109 = 2 \cdot 7^2 + 1 \cdot 7^1 + 4 \cdot 7^0$ $\downarrow$ $(2 \cdot 8^2 + 1 \cdot 8^1 + 4 \cdot 8^0) - 1 = \mathbf{139}$
...	...
$3 \cdot 2^{402653209} - 1$	$3 \cdot 2^{402653210} - 1$
...	...
A very large number	**0**

Table 7. The Goodstein sequence for 4. All b^0's are written out for clarity.

Index	$G(5)$
1	**5**
2	**27**
3	**255**
4	**467**
5	**775**
6	**1197**
7	**1751**
...	...
A very large number	**0**

Table 8. The Goodstein sequence for 5.

comparing two numbers in $G(n)$ is equivalent to comparing their corresponding ordinals in $O(n)$. Because of this bijection, we can prove that $G(n)$ will terminate if and only if $O(n)$ terminates.

We define a function $f(n, b)$ that first determines the hereditary base-b representation of n and replaces every b appearing in the representation with ω. For example,

$$f(123, 2) = f(1 \cdot 2^{2^2+2^1} + 1 \cdot 2^{2^2+1} + 1 \cdot 2^{2^2} + 1 \cdot 2^{2^1+1} + 1 \cdot 2^1 + 1, 2) = \omega^{\omega^\omega+\omega^1} + \omega^{\omega^\omega+1} + \omega^{\omega^\omega} + \omega^{\omega^1+1} + \omega^1 + 1 \tag{4.1}$$

and

$$f(123, 3) = f(1 \cdot 3^{3^1+1} + 1 \cdot 3^{3^1} + 1 \cdot 3^2 + 2 \cdot 3^1, 3) = \omega^{\omega^1+1} + \omega^{\omega^1} + \omega^2 + \omega \cdot 2 \tag{4.2}$$

Note that we must take care to put the larger terms on the left and write $2 \cdot \omega$ as $\omega \cdot 2$ to avoid, once again, the non-commutativity of ordinal arithmetic.

For the sequence $O(n)$, each ith term $O(n)_i$ is defined to be $f(G(n)_i, i+1)$. Returning to our 123 example, the third term of $O(123)$, $O(123)_2$, is $f(G(123)_2, 3)$, or $\omega^{\omega^1+1}+\omega^{\omega^1}+\omega^2+\omega\cdot 2$.

Let $G'(n)_i$ be $G(n)_i$ after applying the base-changing operation to generate the next element but before subtracting 1. This means that $G(n)_{i+1} = G'(n)_i - 1$ and $f(G(n)_i, i + 1) = f(G'(n)_i, i + 2)$. Then, after doing the subtracting one operation on the left, we get $f(G(n)_{i+1}, i+2) - 1 = f(G'(n)_i, i+2)$, and therefore, $f(G(n)_{i+1}, i+2) < f(G'(n)_i, i+2)$. In other words, every $i+1$th element in the Goodstein sequence of n will always be strictly less than the ith element of the same sequence, even if written in a different base. As such, we have proven that the sequence $O(n)$ must be strictly decreasing. Because an infinite strictly decreasing sequence of ordinals cannot exist (see above Gentzen's proof) and all decreasing sequences of ordinals must terminate, then $O(n)$ must terminate, and because there is a bijection between $O(n)$ and $G(n)$, this means that $G(n)$ must also terminate, and reach 0. ■

4.5. **Proof of Goodstein's theorem's nonexistence under Peano arithmetic: the Kirby-Paris theorem.** The proof of the Kirby-Paris theorem of how Goodstein's theorem cannot be proved under Peano arithmetic is significantly more difficult and cannot be easily described here. The reader is referred to the references and especially [KP82].

5. Significance of ordinal proofs

For both of the proofs presented above, the key feature that made ordinals so powerful was a demonstration of the contradictions that arise from ordinal association due to the impossibility of an infinitely decreasing set of ordinals. This is an extremely powerful tool, and ordinal arithmetic is appropriately considered a second-order mathematical system (one that talks about sets) above first-order Peano arithmetic (one that only talks about individual elements). Yet the very powerful nature in the way that we have defined ordinals brings along with it some axioms that are unprovable. The nature of infinity in mathematics itself is controversial, and simply declaring an order, while intuitive to the minds of some humans, may not fully convince others of their full mathematical rigor. The greatest challenge in proving the most basic abstract ideas in all of math is the fact that underneath every mathematical system, it is impossible to know for sure whether your very first initial assumptions are true, even a simple one like "The empty set exists."

Gentzen's proof highlights how beyond the simple mathematical systems that we've used day-to-day, there are other systems in which certain truths are clearer or less clear based on the initial assumptions that that system makes, similar to how Lobachevsky showed how

Euler's fifth axiom was more optional than originally perceived, bringing forth hyperbolic and Lagrangian geometry. Goodstein's theorem shows us how, for a remarkably and deceivingly simple set of rules, one can construct a mathematical problem that cannot be declared true without going above what we know to be true and making some more assumptions in the land of ordinal arithmetic. Perhaps more unsolved questions and conjectures may be provable in ordinal arithmetic than we may originally perceive.

A final question for the reader to ponder: what would happen if we defined well-ordered ordinal sets to require a greatest element instead of a least element? Would things reverse in the way we would want them to?

6. Final Thanks

A big thanks to Simon Rubinstein-Salzedo and all the TAs for allowing Euler Circle to exist and providing opportunities for young students to receive guidance in writing mathematics papers. Additional thanks to Lisa Liu for reading over, providing guidance, and suggesting changes to a first-attempt at a paper written by a high-schooler without prior experience in the field of abstract math.

References

[Gen35] Gerhard Gentzen. Untersuchungen über das logische schließen. ii. *Mathematische zeitschrift*, 39, 1935.

[Gen36] Gerhard Gentzen. Die widerspruchsfreiheit der reinen zahlentheorie. *Mathematische annalen*, 112(1):493–565, 1936.

[Göd65] Kurt Gödel. On formally undecidable propositions of principia mathematica and related systems i. *The Undecidable*, pages 5–38, 1965.

[Goo44] Reuben Louis Goodstein. On the restricted ordinal theorem. *The Journal of Symbolic Logic*, 9(2):33–41, 1944.

[HJ99] Karel Hrbacek and Thomas Jech. *Introduction to set theory, revised and expanded.* Crc Press, 1999.

[Kle52] Stephen Cole Kleene. Introduction to metamathematics. 1952.

[KP82] Laurie Kirby and Jeff Paris. Accessible independence results for peano arithmetic. *Bulletin of the London Mathematical Society*, 14(4):285–293, 1982.

[Kre71] Georg Kreisel. The collected papers of gerhard gentzen., 1971.

[Rat15] Michael Rathjen. Goodstein's theorem revisited, 2015.

[Sie58] Wacław Sierpiński. *Cardinal and ordinal numbers*, volume 1958. Warszawa, 1958.

[W$^+$12] Raymond L Wilder et al. *Introduction to the Foundations of Mathematics*. Courier Corporation, 2012.

[Wei04] Eric W Weisstein. Hilbert's problems. *https://mathworld. wolfram. com/*, 2004.

Email address: 25stu567@lexingtonma.org