BEYOND INFINITY 5: LARGE NUMBERS AND BIG THEOREMS

JADE NINE

1. Large Ordinals

We have been introduced to the ordinal $\mathfrak{c}$. $\mathfrak{c}$ is the cardinality of $\mathcal{P}(\omega)$. It is an uncountable ordinal. ω cannot *reach* it - any function from ω into $\mathfrak{c}$ must stop short before it covers all of $\mathfrak{c}$, it cannot possibly cover the whole thing. So $\mathfrak{c}$ is an uncountable ordinal.

There is another very large ordinal: the smallest uncountable ordinal. For this one, we use the symbol ω_1, pronounced "omega one". The familiar ω, by contrast, is sometimes called ω_0. Formally, $\omega_1 = \{t \in \mathfrak{c} \big| |t| = \omega\}$. This is a valid definition; and indeed, because ω_1 contains all countable ordinals and no ordinal ever contains itself, ω_1 must not contain itself, and therefore must not be countable. Yet, clearly, any smaller ordinal is countable, because any smaller ordinal *is* an element of ω_1. Thus, ω_1 is the smallest uncountable ordinal. Why is it very big? It is so big that it can only be described by the axiom of separation, not a constructive axiom like $\omega = \{0, 1, 2, 3, ...\}$. We'll see why this is significant next week when we collapse cardinals.

Anyways, now that we have ω_1, we can now manipulate cardinality to do some more bizarre but fascinating things. Let's talk about trees!

Before we do, though, I will give you a large countable ordinal to think about:

Definition 1 (ε_0)**.** Define ordinal exponentiation as follows: for limit ordinals α, the exponential β^α is equal to $\bigcup\{\beta^t \big| t \in \alpha\}$. Then take the sequence ω, ω^ω, $\omega^{(\omega^\omega)}$ (commonly written as ω^{ω^ω}), $\omega^{\omega^{\omega^\omega}}$, ... The limit of this sequence is called ε_0, pronounced "epsilon naught" (naught means zero).

2. Trees

Definition 2 (Branch)**.** A branch of a poset is a maximal well-ordered subset of the poset (maximal means that it's not part of a bigger branch).

Definition 3 (Tree)**.** A tree is a poset P such that, $\forall x \in P$, $O(x)$ is well-ordered. Trees, by this definition, are comprised of branches, but may have many separate branches.

Definition 4 (Level)**.** Given some ordinal α, the α-level of a tree is the set of all elements of the tree whose segment has order type α.

Definition 5 (Height)**.** The height of a tree is the smallest ordinal α such that the tree is all entirely below the α-level.

Here's an example of a tree: put one node at the 0-level, and then put ω many nodes at the 1-level. What you get is a short but branchy tree. Here's another: put one node at each n-level for all $n \in \omega$. What you get is a tall but not-very-branchy tree (it only has one branch).

Each level consists of incomparable elements (because otherwise they wouldn't all be able to have the same ordinal as their segment's order type), so to some extent, the size of each level represents the amount of branching that the tree is doing.

Here's another tree: collect a branch of size n for each $n \in \omega$, and then connect them at the root, to get a tree. This tree has infinitely many branches, but each branch is finite. We have thus found a tree whose height is infinite, and in fact the number of elements of the tree is infinite, but each branch is finite. However, notice this: each level, after the 0-level, is infinite. Take the 1-level: it has a node from every branch in the tree, and there are infinitely many branches, thus this level is infinite.

Here's a fun theorem.

Theorem 1 (Wandering Trees)**.** *Every tree of height ω has an infinite branch or an infinite level.*

Proof. This is possible to prove by contradiction: let's suppose the tree has all levels and branches finite. Then, start at the root, and travel a path going upwards - each time you move up, pick a node that has infinitely many nodes (elements) above it. This is always possible, because if there are infinitely many nodes above a node, but only finitely many nodes at the next level, one of those nodes at th next level must lead to an infinite tree above it. Essentially, move up by picking

Date: July 26, 2020.

the 'most promising' choice at each step. You will end up traveling infinitely far, because there are always infinitely many possible destinations above you, thus you can never run out of choices to move up. But, your infinite travel is an infinite branch. This is a contradiction. □

And with that, I will now introduce to you the wonderful Aronszajn tree.

Theorem 2 (Aronszajn Tree)**.** *There exists a tree of height ω_1 whose branches and levels are all countable.*

Proof. One can actually explain how to put together an Aronszajn tree; to do so, we'll need a few useful processes. The first is the idea of a partial function - a partial function on a domain x is a function whose domain is a subset of x. The range of a partial function is considered, as usual, to just be all elements that f maps to.

Then, we have an ordering on partial functions: let $f < g$ if $dom(f) \subset dom(g)$ and $\forall x \in dom(f)(f(x) = g(x))$. The function g is said to be an *extension* of f; it does everything f does, plus some more.

Then, there is the concept of finite equivalence. Consider two partial functions f, g to be finite-equivalent if $dom(f) \triangle dom(g)$ is finite and $f(x) = g(x)$ for all but finitely many x in $dom(f) \cap dom(g)$. The idea is that f and g 'agree' in all but finitely many places.

Lastly, I will use a concept call coinfinity: a subset S of ω is said to be coinfinite if its complement $\omega \setminus S$ is infinite. Then, a partial function f on ω is said to be coinfinite if its domain is coinfinite.

The actual construction of the tree is left as a homework problem. □

Now for a change of pace.

3. Russell's Paradox and Related Arguments

There is a famous paradox involving axiomatic set theory, that goes as follows:

Let s be the set of all sets that do not contain themselves. Then, does s contain itself?

- If $s \in s$, then s contains itself, thus by its own requirement, it is not in itself. This contradicts $s \in s$.
- If $s \notin s$, then s does not contain itself, thus by its own requirement, it is in itself. This contradicts $s \notin s$.

It's a perfectly sound logical paradox. It's because of this paradox that we can't have a set of all sets. If we did, we could do something similar to the above using our axiom of separation, and end up in trouble. This is why the axiom of separation restricts itself to subsets of sets that already exist: you can't simply collect all sets in the entire universe that satisfy a certain property.

This spirit of setting up a definition of an object that contradicts its own definition is actually useful in other theorems. In an indirect way, the concept of Russell's Paradox is a key argument to understand in set theory.

Here are two theorems that use an argument of a similar spirit.

Theorem 3 (Cantor's Diagonal Argument)**.** *For any nonempty set x, $|\mathcal{P}(x)| \neq |x|$.*

Proof. We will prove this by contradiction. Suppose that, for some set x, there does exist a bijection $f : x \to \mathcal{P}(x)$. What I'll now do is collect the set of all elements of x that are not contained in the set named after them. Formally, like this: let $a = \{t \in x | t \notin f(t)\}$. Remember that f is a function that sends elements of x to subsets of x, so $t \notin f(t)$ makes sense.

Notice that a is itself a subset of x. Therefore $a \in \mathcal{P}(x)$, i.e. a is in the range of f. Because f is a bijection, there must therefore be an inverse value of a, namely some element $f^{-1}(a) \in x$. Let this element be called b, that is, $b = f^{-1}(a)$.

Now, is b an element of $f(b)$?

I'll let you finish the argument from here. □

The next theorem is perhaps one of the most famous in formal logic. It is extremely important, for math in general, and for understanding how truth relates to provability. It is a rather involved logical argument, but I've simplified it to capture the core idea.

Theorem 4 (Gödel's First Incompleteness Theorem)**.** *There is a logical statement that is neither provable nor disprovable.*

The setup is this: suppose that all logical statements - including theorems, axioms, formulas, and all the rest - have a name. I will take advantage of this in the following manipulation: let $Sb(x)$ be the statement that you get by taking a logical statement x and replacing its first free variable with the name of x itself (free variable means there is no $\forall$ or $\exists$ in front of it). Then, let $Q(x, y)$ be the statement "x is a name for a proof of $Sb(y)$". Indeed, given the name of a statement, one can pull up the statement, read it, then check it against $Sb(y)$, and confirm whether or not it's a proof of $Sb(y)$. Lastly, let p be the name of the statement $\forall x(Q(x, y))$. Then $Sb(p)$ is true but not provable.

Proof. If $Sb(p)$ is provable, then we deduce that $Sb(p)$ is true (because it can be proved to be true); note that $Sb(p) = \forall x(Q(x,p))$, thus $\forall x(Q(x,p))$ is true. But $Q(x,p)$ means that x is not a name for a proof of $Sb(p)$, thus $\forall x(Q(x,p))$ means that there is no name for any proof of $Sb(p)$. This contradicts the notion that $Sb(p)$ is provable in the following way: if $Sb(p)$ has a logical proof, then that proof has a name.

If $Sb(p)$ is disprovable, then it is false. But this is a problem: we deduce that, because $Sb(p) = \forall x(Q(x,p))$, then $\forall x(Q(x,p))$ is false. Therefore $\exists x(\neg Q(x,p))$ is true. But $\neg Q(x,p)$ means that x *is* the name of a proof of $Sb(p)$. Thus $\exists x(\neg Q(x,p))$ means that there is some name that corresponds to a proof of $Sb(p)$. But this contradicts the notion that $Sb(p)$ is false in the following way: you can't prove false statements. □

4. Formal Logic and Proof Theory

A theory is a collection of axioms, together with rules of mathematical logic, that can be used to deduce other logical statements.

Zermelo-Fraenkel Set Theory Plus The Axiom of Choice, abbreviated ZFC, is the theory that consists of the axioms presented in this course, together with the standard symbolic logic using symbols $\vee, \wedge, \implies, \iff, \neg, =$.

A deduction is a logical statement of the form "$p \implies q$ and p is true, therefore q is true".

A proof is a collection of deductions that begins at the axioms of a theory and ends up in a desired statement. The proof is said to be a *proof of* the result statement.

A theory is said to prove a statement if there is a proof of that statement using the axioms and logic of the theory.

A contradiction is a statement that violates the laws of logic that are being used in the theory. For example, $p \wedge (\neg p)$ is a contradiction. so is $x \neq x$.

A theory is consistent if it cannot prove any contradictions.

A theory is inconsistent if it *can* prove a contradiction. For example, ZFC together with the axiom $\emptyset = \{\emptyset\}$ is a contradiction, because anything in the empty set is (by definition) not equal to itself; we can then use the axiom of extensionality on $\emptyset = \{\emptyset\}$ to deduce that $\emptyset \in \emptyset$ and therefore $\emptyset \neq \emptyset$, which is a contradiction.

Lastly, you are allowed to add axioms or statements to a theory to make a new theory. Such a process is usually written using the + symbol, so for example, if ZF refers to ZFC without the Axiom of Choice, then ZFC = ZF + Axiom of Choice. This process is called extension. Thus, ZFC is an extension of ZF. Be careful: even if the base theory you start with is consistent, the extension might not be - as we saw above, even if ZFC is consistent, ZFC + $(0 = 1)$ is definitely inconsistent.

Gödel's First Incompleteness Theorem means that, given any theory, there are statements that are neither provable nor disprovable in that theory. This is assuming that the theory is consistent.

The statement $Sb(p)$ from Gödel's theorem is true (review the proof to see why it's a problem if $Sb(p)$ is false), so here is an example of a statement that is true but not provable.

ZFC is believed to be consistent. When I say 'believed' to be consistent, why is it that we can't *prove* that the theory is consistent? Well, it turns out, you can extend Gödel's First Incompleteness Theorem to get an argument that no theory can prove its own consistency; this is Gödel's Second Incompleteness Theorem, and I won't present the argument here, but the important point is that any theory, as long as it really actually is consistent, cannot prove its own consistency.

To wrap up, this: at first glance, Gödel's theorem itself is a proof of $Sb(p)$ (review the theorem to understand why it disproves "$Sb(p) is false''$).$So then why is it that$Sb(p) is not provable if Gödel's theorem is itself a proof of $Sb(p)$? It turns out that the catch is that "$Sb(p)$ is disprovable, therefore it is false" cannot be deduced within a theory unless you actually have the disproof at your disposal. This is why Gödel's theorem is not a proof within the theory itself: basically, a theory itself cannot say "a proof exists, therefore the result is true"; it has to actually produce the proof.

5. Independence

We are now ready to discuss logical independence, one of the core advanced logical concepts of this course. Suppose we have a consistent theory, such as ZFC (which is believed to be consistent), and some statement x that can neither be proved nor disproved. Let's try to add x to our base of knowledge: we will extend ZFC by taking x as an axiom. The problem is, we don't know whether it would be more correct to take x or $\neg x$ as the axiom. Indeed, if neither x nor $\neg x$ can be proved, one might guess that each option is equally valid. So, what can we do?

Well, if ZFC+x ends up being inconsistent, clearly it would be correct to take $\neg x$ as the axiom. On the other hand, if ZFC+$\neg x$ ends up being inconsistent, then we need to take x as the axiom.

But, if both ZFC+x and ZFC+$\neg x$ are consistent, then there is no way to know which one of x or its opposite makes for a better axiom. Such a statement is said to be independent of ZFC.

Here is your first example of an independent statement.

Axiom 6 (Continuum Hypothesis)**.** $\mathfrak{c} = \omega_1$

6. Real Numbers

Let's wind down with a concept you are probably familiar with: the real numbers. The real numbers, written as $\mathbb{R}$, are numbers expressed as potentially infinitely long numbers (using a decimal point); there are many popular ways to define the real numbers, but we will do so as follows: any finite or infinite sequence of 1s and 0s, with a decimal point to separate the integer part from the fractional part, is a real number, so long as the integer part of the sequence is finite. Negative real numbers are also allowed, to write these we just use a minus sign. We also remove all unnecessary 0s, so for example to express 00.0100 as a real number, we just write 0.01. This is, in essence, the binary representations of the real numbers.

To be perfectly careful, I have to disallow numbers that contain an infinite sequence of consecutive 1s, but this is just a minor technical point, so don't worry about it.

Also, when I say infinite sequence, strictly speaking I mean a sequence of order type ω - so, you can't have ω many 0s and then a 1 at the end, that's not allowed.