Math 145a - Set Theory I

Taught by William Boney
Notes by Dongryul Kim

Fall 2016

This course was taught by William Boney. We met on Tuesdays and Thursdays from 1:00pm to 2:30pm. We used *Set Theory: The Independence Phenomenon* by Peter Koellner as a textbook. There were 15 people enrolled in the course. Grading was based on 60% weekly homeworks, 20% in-class midterm, and 20% three-hour final. The course assistance was Justin Cavitt.

Contents

1 September 1, 2016

Because it's hard to start from the very bottom, I am going to start with three motivating problems.

1.1 Three problems

The **cardinality** of X is the number of elements in X. For instance we are going to say that $|X| = |Y|$ if there is a bijection $f : X \to Y$.

Theorem 1.1. *For every X, its power set $\mathcal{P}(X) = \{Y : Y \subseteq X\}$ has greater cardinality than X.*

An immediate corollary is that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$. This leads to a question that comes from Cantor: is there anything between them? This fundamental problem was left open until it was answered as not an answer. The statement is independent of ZFC, i.e., the foundations of ZFC is just not enough to answer this problem. The **continuum hypothesis** states that the answer to this is no, and the generalized continuum hypothesis deals with the existence of sets Y with $|X| < |Y| < |\mathcal{P}(X)|$ for an arbitrary set X.

The second problem is about combinatorics. The ordered set $(\mathbb{R}, <)$ can be characterized by (1) dense linear ordering without endpoints, (2) connected in the order topology, and (3) separable in the order topology. Now Suslin's question was whether one can replace the third condition (3) to (3') every collection of disjoint open intervals is countable. The answer to this is again, who knows?

The word combinatorics is used here because such questions are related to trees, or proper generalization of trees.

Lemma 1.2 (König's lemma)**.** *If T is an infinite tree such that every vertex has finitely many neighbors, then there is an infinite path through T.*

One thing set-theorists like to do is to take a true statement and ask what happens when objects get larger and larger. It fails on the next one. This is basically because there is this nice countable dense set $\mathbb{Q}$. But things get interesting when we take it to the next step. Then the independence phenomenon comes in to the picture.

The third theme is measure theory. This is the measure theory in the actual measure theoretic sense.

Theorem 1.3. *(1) (Vitali) There are non-measurable sets.*
(2) (Banach-Tarski) You can decompose one sphere and reassemble them into two spheres of equal volume.

One of my friends use the Banach-Tarski theorem to give a physical proof of the negate of the axiom of choice. But I don't accept this proof. There is a good reason we can't do this in nature, and it's because they never occur in the physical world. This is related to the hierarchy of sets in descriptive set theory.

1.2 Functions and pairs

"All the world's a set, and all mathematicians and theorems merely elements."
—William Setspeare

Every mathematical object is built out of sets, and those elements are all set. So in fact, every thing can be written in curly braces and commas.

As an example, how do we encode a function $f : A \to B$ as sets? We can think it as a set of ordered pairs

$$f = \{(a, f(a)) : a \in A\}.$$

This is also called the graph of f but is actually just f.

But to do this, we need to know what ordered pairs are. Given x, y, we want a set (x, y) such that $(x, y) = (a, b)$ if and only if $x = a$ and $y = b$. We define

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

You will work this out in you homework. One thing to watch out is when $x = y$.

1.3 Natural numbers to real numbers

We are not going to construct the natural numbers $\mathbb{N}$, which starts with 0 in this course. We define

$$0 = \{\} = \emptyset.$$

The next number is 1. We're going to define 1 to be

$$1 = \{\emptyset\} = \{0\}.$$

Then we define $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$ and so on. Given n, we are going to define

$$n + 1 = n \cup \{n\}.$$

Then the natural numbers is $\mathbb{N} = \{n : n \in \mathbb{N}\}$ although it looks silly. We define $n < m$ if and only if $n \in m$. Likewise we can say that $n \leq m$ if and only if $n \subseteq m$. Here, $X \subseteq Y$ is defined as $\forall x(x \in X \to x \in Y)$.

To define $n + m$, we need more than just elements. We are going to define $n+m$ as the unique k such that there is a bijection from k to $(\{0\}\times m)\cup(\{1\}\times n)$. Likewise, we define nm to be the unique k such that there is a bijection from k to $n \times m$.

Now we get to the integers $\mathbb{Z}$. Now there is a standard way to make a monoid into a group, in algebra. For $(m, n) \in \mathbb{N}^2$, we want this to represent $m - n$. But because we don't know subtraction yet, we set

$$(m, n) \sim (m', n') \quad \text{if and only if} \quad m + n' = m' + n.$$

This is in fact an equivalence relation. So we define

$$\mathbb{Z} = \{[(m, n)]_\sim : (m, n) \in \mathbb{N}^2\}.$$

If you have in mind what (m, n) represents, it is not hard to extend addition and multiplication. We define

$$[(m,n)]_\sim + [(m',n')]_\sim = [(m+m', n+n')]_\sim,$$
$$[(m,n)]_\sim \cdot [(m',n')]_\sim = [(mm'+nn', mn'+m'n)]_\sim.$$

In a similar way, we can construct the rationals. This is just turning a ring into the field of fractions. For $(a,b),(c,d) \in \mathbb{Z}^2$ with $b,d \neq 0$, we define an equivalence relation

$$(a,b) \sim (c,d) \text{ if } ad = bc.$$

Then we can define the equivalences classes as $\mathbb{Q}$. We end up with

$$[(a,b)]_\sim + [(c,d)]_\sim = [(ad+bc, bd)]_\sim.$$

Lastly I want to talk about the reals mainly because I have put a problem about the reals in the problem set. You could give a metric and then define the Cauchy sequences as real numbers, but the way I am going to do is through Dedekind cuts. Say that $L \subseteq \mathbb{Q}$ is **proper downward closed** if $\emptyset \neq L \neq \mathbb{Q}$ and for any $x < y \in \mathbb{Q}$ if $y \in L$ then $x \in L$. Define $L_0 \sim L_1$ if they have the same supremum, which can be written as "for any $x \in L_0$ and $n \in \mathbb{N}$ there exists a $y \in L_1$ such that $x - 1/n < y$ and vice versa." Then we let

$$\mathbb{R} = \{[L]_\sim : L \subseteq \mathbb{Q} \text{ proper downwards closed}\}.$$

The equivalence relation is to take care of $(-\infty, 0) \sim (-\infty, 0]$.

2 September 6, 2016

We're going to define Zermelo-Fraenkel set theory with Choice. There will be two types of axioms. The first will be that certain sets exist. The second type will be that we can get some sets from other sets. To deal with sets, we are going to use a single binary relation $\in$ (and $=$), which intuitively means "member of".

2.1 Zermelo-Fraenkel with Choice

This is just a list of axioms.

Axiom of Extensionality.

$$\forall x, y, [x = y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y)]$$

That is, sets are made up of elements.

We are going to define $x \subseteq y$ to mean

$$\forall z(z \in x \to z \in y).$$

So we can restate the Axiom of Extensionality as

$$\forall x, y, [x = y \leftrightarrow (x \subseteq y \wedge y \subseteq x)].$$

Axiom of Empty set.

$$\exists a \forall x(x \notin a)$$

That is, there is an empty set, which we will denote $\emptyset$.

Axiom of Pairing.

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

If x, y are sets, so is $\{x, y\}$.

This implies that because $\emptyset$ is a set, $\{\emptyset\}$ is also a set.

Axiom of Union.

$$\forall x \exists a \forall z(z \in a \leftrightarrow \exists y(z \in y \wedge y \in x))$$

This a is denoted $\bigcup x$.

This is a bit different from what we are used to, because $\bigcup_{i \in I} X_i$ is what we now defined as $\bigcup\{X_i : i \in I\}$. In a little bit, we will justify this. We will need to think about why the set of X_i is a set.

Axiom of Power Set.

$$\forall x \exists \mathcal{P}(x) \forall x(z \in \mathcal{P}(x) \leftrightarrow z \subseteq x)$$

$\mathcal{P}(x)$ is the collection of all *subsets of x.*

This is what justifies talking about its subsets, like in defining a topological space. This also says that you can get all of the subsets of x, no matter how huge x is.

Axiom of Infinity.

$$\exists a(\emptyset \in a \wedge \forall y(y \in a \to y \cup \{y\} \in a)$$

There is a set that contains all the "natural numbers".

It would be nice to show that $y \neq \{y\}$. The next axiom will help us out here. We note that we haven't actually justified that the set of natural numbers is a set.

Now this was what Zermelo came along when Russel found a problem. People were happy for a while but there were still problems and Fraenkel added this single axiom on top of Zermelo's system.

Axiom of Foundation/Regularity.

$$\forall x[x \neq \emptyset \to \exists y(y \in x \wedge \forall z(z \in x \to z \notin y))]$$

You can show that this is equivalent to $\neg(\exists\{x_n : n \in \mathbb{N}\}(x_{n+1} \in x_n))$.

A **formula** is going to be $\varphi(x_1, \ldots, x_n)$ and built from

- $x_i \in x_j$ and $x_i = x_j$,
- using logical symbols $\to$, $\wedge$, $\vee$, $\neg$,
- using quantifiers $\exists$, $\forall$.

This is called first order logic, and the beauty of set theory is that everything is first order logic, because of the Axiom of the Power Set and the other axioms.

Replacement Schema. *For every $\varphi(x, y, z_1, \ldots, x_n)$, include*

$$\forall a_1, \ldots, a_n \forall a[\forall y \in a \exists! z \varphi(y, z, a_1, \ldots, a_n) \to \exists b \forall z(z \in b \leftrightarrow \exists y \in a \varphi(y, z, a_1, \ldots, a_n)]$$

If $\varphi(x, y, a_1, \ldots, a_n)$ defines a function with domain a, then its image is a set.

We can't write this as a single axiom for metamathematical reasons. Although ZFC looks like a finite list of axioms, it is not because this is a schema. It gives an axiom for every formula.

Axiom of Choice.

$$\forall x[\forall y(y \in x \to y \neq \emptyset) \to f \textit{ a function with domain } x(\forall y \in x(f(y) \in y))]$$

There are instances when picking a choice function becomes easy. The first is when there are a finite number of sets. The second is when the sets have some additional structure so that you can find a certain element easily. You need the Axiom of Choice when you are picking among an infinite pair of socks but you don't need it when you are picking among an infinite pair of shoes, because you can choose the left one.

2.2 Equivalents of Replacement

There is an equivalent formulation of the Replacement Schema that I want to talk about.

Comprehension.

$$\forall a_1, \ldots, a_n \forall a \exists b \forall x (x \in b \leftrightarrow (x \in a \wedge \varphi(x, a_1, \ldots, a_n))$$

This means that if you have a set, then the elements in there that satisfies something is also a set.

Collection.

$$\forall a_1, \ldots, a_n \forall a [y \in a \exists! z \psi(y, z, a_1, \ldots, a_n) \to \exists b \forall z (y \in a \psi(y, z, a_1, \ldots, a_n) \to z \in b)]$$

This means that if you have some function then there is the set that contains the image.

Now if you have both Comprehension and Collection, then you can get Replacement by just taking the set that contains the image and restricting it to the actually image using Comprehension. It is also easy to see that Replacement implies Collection.

Proposition 2.1. *Under the other axioms of ZF, the Replacement Schema implies the Comprehension Schema.*

Proof. Take a and $\phi(x, a_1, \ldots, a_n)$. If $\neg\varphi(e, a_1, \ldots, a_n)$ for all $e \in a$, then we are done since what we want is the empty set. If not, let $e \in a$ be a witness. Define $\psi(x, z, a, e, a_1, \ldots, a_n)$ to be

$$[x \in a \wedge \varphi(x, a_1, \ldots, a_n) \to x = z] \wedge [\neg(x \in a \wedge \varphi(x, a_1, \ldots, a_n)) \to z = e].$$

Then this ψ does what we want to do in Replacement. □

2.3 Basic notions

We are still in a very clunky stage because we don't have a lot of tools we used to have.

Given x, y, we define the **intersection** as

$$x \cap y = \{a \in x : a \in y\}.$$

We also can define the ordered tuple as

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

For n-tuples, we define $(x_1, x_2, x_3) = ((x_1, x_2), x_3)$ and iterate this process.

We can now define the **product** as

$$X \times Y = \{(x, y) \in \mathcal{P}(\mathcal{P}(X \cup Y)) : x \in X \wedge y \in Y\}.$$

Then we can define functions too.

Definition 2.2. A set f is a **function** if there exists X, Y such that $f \in \mathcal{P}(X, Y)$ such that for all $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in f$. We are going to write this as $f(x) = y$ because we are mathematicians.

3 September 8, 2016

By Union, we know that $\bigcup x = \bigcup_{y \in x} y$ is a set. So if $\{X_i : i \in I\}$ is a set, then

$$\bigcup_{i \in I} X_i = \bigcup \{X_i : i \in I\}$$

is a set.

3.1 Classes

Everything we talk about is a set. But we need to distinguish it from the following proposition.

Proposition 3.1. *There is no set of all sets.*

Proof. Suppose x is the set of all sets. Then $x \in x$ contradicts Foundation. Or alternatively $\{y : y \notin y\}$ is a set by Comprehension, and Russel's paradox leads to a contradiction. □

But I'm talking about the collection of sets, by giving a quantifier. A **class** is simply any collection of sets. Clearly any set is a class. A **proper class** is a class that is not a set. **Definable classes** are classes with a first-order definition, and all other classes are called **undefinable classes**.

Example 3.2. The formula $x = x$ defines the class V, which is also called **Von Neumann universe**. Another class is Grp, which is the class of all groups. I can't give an example of an undefinable class, because if I can, then it would be definable.

The reason there are proper classes is because there can be collections that are too big. Suppose a is a set and $\mathcal{X}$ is a class such that there is a bijection $f : a \to \mathcal{X}$. Here f is not really a set but a definition of a function. Then by Replacement, $\mathcal{X}$ is a set.

3.2 Axiom of Choice

Let us recall that this axiom says that

$$\forall x(\forall y(y \in x \to y \neq \emptyset) \to \exists \text{function } f \text{ with dom. } x \text{ s.t. } \forall y(f(y) \in y)).$$

Definition 3.3. A relation $<$ on X is called a **well-ordering** if and only if

- $\forall x, x \not< x$.
- $\forall x, y, x < y$ or $x = y$ or $y < x$.
- $\forall x, y, z, (x < y$ and $y < z \to x < z)$.
- $\forall \emptyset \neq Y \subseteq X, \exists y \in Y$ s.t. $\forall z \in Y(y < z$ or $z = y)$.

An example of a well-ordering is $(\mathbb{N}, <)$. This is actually equivalent to induction.

Theorem 3.4. *The following are equivalent in ZF.*

(1) The Axiom of Choice.

(2) Every set can be well-ordered.

(3) The product of nonempty sets is nonempty.

(4) For all x, y, either $|X| \leq |Y|$ or $|Y| \leq |X|$.

Given a collection $\{X_i : i \in I\}$, what is $\prod_{i \in I} X_i$? Some element $x \in \prod_{i \in I} X_i$ should associate to a function that picks an element of x_i for each $i \in I$.

Proof of (2) $\to$ (1). Let $\{X_i : i \in I\}$ with $X_i \neq \emptyset$. We are going to well-order this set, and then there is a unique element we can pick, which is the minimal element. Set

$$X^* = \bigcup \{X_i : i \in I\}$$

and let $<^*$ be a well-order of X^*. Then define f by $f(i) = \min X_i \in X_i$. This is a choice function. $\square$

There are some weakenings of the Axiom of Choice, and one of this is the Axiom of Dependent Choice.

Axiom of Dependent Choice. *Let R be a relation on X such that for all $x \in X$ there exists a $y \in X$ such that xRy. Then there exists a set $\{x_n \in X : n \in \mathbb{N}\}$ such that $x_n R x_{n+1}$.*

You can of course do this finitely many times with ZF, but you run out of time as you try to do it infinitely many times. That is why you need this axiom. This is sometimes used in other areas of mathematics like analysis.

3.3 Cardinality of sets

We want to use the cardinal $|X|$ is an emblem representing the size of X. Likewise, we want to use ordinals to represent a specific order type.

Theorem 3.5 (Cantor)**.** *For every set X, thre is not surjection from X to $\mathcal{P}(X)$. Here, $f : X \to Y$ is a surjection if and only if for all $y \in Y$ there exists an $x \in X$ such that $f(x) = y$.*

Proof. Suppose $f : X \to \mathcal{P}(X)$ was a surjection. Define

$$D = \{x \in X : x \notin f(x)\} \in \mathcal{P}(X).$$

By surjectivity, there exists an $a \in X$ such that $f(a) = D$. If $a \in D$, then $a \notin f(a)$, so $a \notin D$. If $a \notin D$, then $a \notin f(a)$, so $a \in D$. $\square$

This leads us to talking about sizes of sets.

Definition 3.6. Fix X and Y that are nonempty. We write:

- $|Y| \geq |X|$ if there exists a surjection $f : X \to Y$.
- $|X| \leq |Y|$ if there exists an injection $f : X \to Y$.
- $|X| = |Y|$ if there exists a bijection $f : X \to Y$.

For example, $|X| \leq |\mathcal{P}(X)|$ and $|X| \neq |\mathcal{P}(X)|$. Also, we have

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{Q}[X]|.$$

These are called **countable sets**. Also,

$$|\mathbb{R}| = |\mathbb{C}| = |\mathcal{P}(\mathbb{N})|$$

and this is called the continuum.

The $\leq$ and $\geq$ symbols are not order relations. The whole thing $|X| \geq |Y|$ is just one symbol. So we may want to ask a few questions.

(1) Is $|Y| \leq |X|$ equivalent to $|X| \geq |Y|$?

(2) Does $|X| \leq |Y|$ and $|Y| \leq |X|$ imply $|X| = |Y|$?

(3) What is $|X|$?

(4) For every X, Y, is it true that either $|X| \leq |Y|$ or $|Y| \leq |X|$?

Proposition 3.7. *The answer to (1) is yes!*

Proof. Suppose $f : Y \to X$ is injective. Let $y_0 \in Y$ and set $g : X \to Y$ by

$$g(x) = \begin{cases} y & \text{if } x = f(y) \\ y_0 & \text{else.} \end{cases}$$

This is a surjective function.

Now suppose that $g : X \to Y$ is a surjection. Put a well-ordering $<$ on X and define $f : Y \to X$ by $f(y) = \min g^{-1}\{y\}$, where $g^{-1}\{y\}$ is the inverse image. This requires the Axiom of Choice. $\square$

4 September 13, 2016

4.1 Well-founded and well-ordered

As I said, we are going to use ordinals as some kind of emblems. As a prototype for well-foundedness, we use $(V, \in)$.

Definition 4.1. let R be a binary relation on X (possibly definable classes).

(1) R is **strict** if and only if $\neg(xRx)$ for all $x \in X$. Also R is a **linear ordering** if and only if it is transitive, antisymmetric, and for all $x, y \in X$, xRy, yRx, or $x = y$.

(2) The **transitive closure** $TC(R)$ of R is the binary relation on X such that $xTC(R)y$ if and only if $x_1, \dots, _n \in X$ such that $x_1 = x$, $x_n = y$, and $x_i R x_{i+1}$.

(3) Define

$$\mathrm{ext}_R(x) = \{y \in X : yRx\}, \qquad \mathrm{pred}_R(x) = \{y \in X : yTC(R)x\} = \mathrm{ext}_{TC(R)}(x).$$

(4) Given $Y \subseteq X$, Y is R**-transitive** if and only if $x \in Y$ implies $\mathrm{ext}_R(x) \subseteq Y$.

(5) We call that R is **well-founded** if and only if $\mathrm{ext}_R(x)$ is a set for all $x \in X$, and every $\emptyset \neq Y \subseteq X$ has an R-minimal element.

(6) R is a **well-ordering** if and only if it is a strict linear order that is well-founded.

As an example, if yRx means that y gave birth to x, then $\mathrm{ext}_R(x)$ are your parents and $\mathrm{pred}_R(x)$ is the ancestors going up in your family tree.

Example 4.2. The universe $(V, \in)$ is well-founded. Also $(\mathbb{N}, <)$ is well-ordered. Also if we throw in ∞, then $(\mathbb{N} \cup \{\infty\}, <^*)$ with $n < \infty$ for all $n \in \mathbb{N}$ is a well-ordering. In fact, if you have any well-ordering on a set, you can throw in the biggest element to get a new well-ordering.

Suppose I is a set and for all $i \in I$, (X_i, R_i) is a well-ordering such that $i < j$ implies $X_i \subseteq X_j$ and $R_i \subseteq R_j$ and $x \in X_i, y \in X_j - X_i$ implies xR_jy. This is an increasing sequence of well-orderings, in the sense that you are adding a few elements that is bigger than every other thing. Then $(\bigcup_{i \in I} X_i, \bigcup_{i \in I} R_i)$ is well-ordered.

4.2 Transfinite induction

Theorem 4.3 (Transfinite induction)**.** *Suppose R is well-founded on X. If $Y \subseteq X$ such that for every $x \in X$, $\mathrm{pred}_R(x) \subseteq Y$ implies $x \in Y$, then $Y = X$.*

Note that this generalizes the induction we already know. Apply the theorem to $(\mathbb{N}, <)$. Then the predecessor of 0 is empty, and so $0 \in Y$. Then the rest is the same as what we learn as "strong induction".

Proof. Suppose not. Then $Y \subsetneq X$. Let $x = \min_R(X - Y)$. Then because every element R-below x is in Y. Thus $\mathrm{pred}_R(x) \subseteq Y$, and $x \in Y$. $\square$

Theorem 4.4 (Transfinite recursion)**.** *Suppose R is well-founded on X and $G : X \times V \to V$ is a function. Then there exists a unique function $F : X \to V$ such that for each $x \in X$, $F(x) = G(x, F|_{\mathrm{pred}_R(x)})$. (Note that V is all of set theory, so $F|_{\mathrm{pred}_R(x)}$ is also in V.)*

Proof. We first prove uniqueness. Suppose F_1 and F_2 both work. Let

$$Y = \{x \in X : F_1(x) = F_2(x)\}.$$

If $\mathrm{pred}_R(x) \subseteq Y$ then

$$F_1(x) = G(x, F_1|_{\mathrm{pred}(x)}) = G(x, F_2|_{\mathrm{pred}(x)}) = F_2(x),$$

so $x \in Y$. Then by induction, $Y = X$.

Let us now prove existence. For $D \subseteq X$, we call $f : D \to V$ **good** if and only if for every $x \in D$, $\mathrm{pred}_R(x) \subseteq D$ and $f(x) = G(x, f|_{\mathrm{pred}_R(x)})$. If $f_1 : D_1 \to V$ and $f_2 : D_2 \to V$, then $f_1|_{D_1 \cap D_2} = f_2|_{D_1 \cap D_2}$ are equal by uniqueness. Then

$$F = \bigcup\{f : f \text{ is good}\}$$

is a function, because we can first use Comprehension to show that the set of domains with a good function is a set, and then use replacement. We now claim that $\mathrm{dom}\, F = X$. This is because if $f : D \to X$ and $x = \min(X - D)$ then set $g : D \cup \{x\} \to X$ by

$$g(y) = \begin{cases} f(y) & \text{if } y \in D \\ G(y, f|_{\mathrm{pred}_R(y)}) & \text{if } y = x \end{cases}$$

and g is good. Then $\mathrm{dom}\, F = X$by induction. $\square$

Definition 4.5. If (X, R) is a well-ordering, and $x \in X$ then denote

$$I^R_x = (\mathrm{pred}_R(x), R \cap (\mathrm{pred}_R(x) \times \mathrm{pred}_R(x))).$$

We also say that $f : (X, R) \cong (Y, S)$ if $f : X \to Y$ is a bijection and for any $x_0, x_1 \in X$, $x_0 R x_1$ if and only if $f(x_0) R f(x_1)$.

Theorem 4.6 (Compatibility)**.** *Let (X, R) and (Y, S) be well-orderings. Then one of the following happens.*

(a) $(X, R) \cong (Y, S)$.

(b) There exists an $x \in X$ such that $I^R_x \cong (Y, S)$.

(c) There exists an $y \in Y$ such that $(x, R) \cong I^S_y$.

Proof. Let $z \notin Y$. Define $G : X \times V \to V$ by

$$G(x, f) = \begin{cases} \min_S Y - f'' \operatorname{pred}_R(x) & \text{if } f : \operatorname{pred}_R x \to X \text{ and } Y - f'' \operatorname{pred}_R(x) \neq \emptyset \\ z & \text{otherwise,} \end{cases}$$

where $''$ denote the image. By transfinite recursion, we get a $F : X \to V$ such that $F(x) = G(x, F|_{\operatorname{pred}_R(x)})$. Set $A = \{x \in X : F(x) \neq z\}$ and let $f = F|_A$.

Then by induction $f'' \operatorname{pred}_R(x) = \operatorname{pred}_S(f(x))$. Then $x_0 R x_1 \to f(x_0) S f(x_1)$. Since R is linear and strict, we get that $x_0 R x_1$ if and only if $f(x_0) S f(x_1)$ and f is an injection. Now I have three cases.

Case 1. $\operatorname{dom} f = X$ and $\operatorname{im} f = f'' \operatorname{dom} f = Y$.
The $f : (X, R) \cong (Y, S)$ and so f is an isomorphism.

Case 2. $\operatorname{dom} f \subsetneq X$.
Let $x_0 = \min(X - \operatorname{dom} f)$. Then $\operatorname{dom} f = \operatorname{pred}_R x_0$. If $Y - f'' \operatorname{pred}_R x_0 \neq \emptyset$, then

$$G(x_0, f) = \min Y - f'' \operatorname{pred}_R x_0 \neq z$$

so $x_0 \in A = \operatorname{dom} f$. This shows that $f : I^R_{x_0} \cong (Y, S)$.

Case 3. $\operatorname{im} f \subsetneq Y$.
Set $y_0 = \min Y - \operatorname{im} f$. Then as before $\operatorname{dom} f = X$. So $f : (X, R) \cong I^S_{y_0}$. $\square$

5 September 15, 2016

5.1 Ordinals for real

As "emblems for well-ordering", we want them to be canonical, and uniquely representative. Recall that X is $\in$-transitive if and only if $x \in y \in X$ implies $x \in X$.

Definition 5.1. A set α is an **ordinal** if and only if $(\alpha, \in)$ is a well-ordering and α is transitive.

This is a very useful definition, because this is first-order and thus gives a definable class On of ordinals. There is a order on On given by $\in$.

Example 5.2. Clearly $\emptyset \in \mathrm{On}$. If $\alpha \in \mathrm{On}$, then $\alpha \cup \{\alpha\} \in \mathrm{On}$. This is called the successor, and we will denote this $\alpha + 1$. Also if $X \in \mathrm{On}$ then $\bigcup X \in \mathrm{On}$. Using this, we see that $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, and so on, are all ordinals.

We set $\omega = \mathbb{N}$. We haven't proved that this is a set, so we need to show this. Heuristically, a collection is not a set only when it is too big. $\mathbb{N}$ is not that big, so it is going to be a set. Recall that the Axiom of Infinity states that

$$\exists \infty (\emptyset \in \omega \wedge \forall x (x \in \emptyset \to x \cup \{x\} \in \infty)).$$

This set ∞ will contain all the natural numbers, but we don't know what else might be inside. So we use comprehension on the expression

$$\psi(x) = \text{“}x \neq \emptyset \vee (\exists x = y \cup \{y\} \wedge \forall y \in x \exists z \in y (y \neq \emptyset \vee y = z \cup \{z\})\text{”}.$$

Then we can define

$$\omega = \mathbb{N} = \{x \in \emptyset : \psi(x)\}.$$

Why is this what we want? It is clear that if n is a natural number, $n \in \omega$. Conversely, let $x \in \omega$. By the definition of ω, we can write $x = y \cup \{y\}$ unless $x = \emptyset$, and then write $y = z \cup \{z\}$ unless $y = \emptyset$, and so forth. If it hits $\emptyset$ at some point, then this contradicts foundation.

I have another definition for ω. Consider the set

$$A = \{Y \in \mathcal{P}(\infty) : \forall x \in Y (x = \emptyset \vee \exists y \in Y (x = y \cup \{y\}))\}$$

and define $\omega = \bigcap A$.

This is the first limit ordinal. Let us now keep going. We see that $\omega + 1 = \omega \cup \{\omega\}$ is an ordinal, and also $\omega + 2 = (\omega + 1) \cup \{\omega + 1\} = \{0, 1, \dots, \omega, \omega + 1\}$ is an ordinal. This way, we get a $\omega + n$ for all natural numbers n.

Next we would want to construct $\omega + \omega$. How do we do this? We see that $\omega \ni n \mapsto \omega + n$ is a definition of a function. So we can use replacement to get $X = \{\omega + n : n < \omega\}$ as a set. Then you can take $\bigcup X$ as an ordinal, and we write $\omega + \omega = \bigcup X$.

Similarly, we can add many ωs, and so write $\omega + \cdots + \omega = \omega n$. Then we can use the same trick, and define $\omega \cdot \omega = \bigcup \{\omega \cdot n : n < \omega\}$. We can go on still further and get a whole hierarchy.

5.2 Properties of ordinals

Proposition 5.3. *Let $\alpha, \beta \in \mathrm{On}$. The following are equivalent:*

(1) $\alpha \in \beta$ *(*$= \alpha < \beta$*)*

(2) $\alpha \subsetneq \beta$

Proof. Let us first prove (1) $\Rightarrow$ (2). Assume $\alpha \in \beta$. Then by transitivity, $\gamma \in \alpha$ implies $\gamma \in \beta$, and so $\alpha \subseteq \beta$. Also, $\alpha \neq \beta$ by foundation.

Now we prove (2) $\Rightarrow$ (1). Set $\gamma = \min(\beta - \alpha)$. By your homework, $\gamma \in \mathrm{On}$, and so $\alpha = \mathrm{pred}_{\in} \gamma$. Again by your homework, $\alpha = \gamma \in \beta$. $\square$

Theorem 5.4 (Linearity)**.** *For all $\alpha, \beta \in \mathrm{On}$, $\alpha \leq \beta$ or $\beta \leq \alpha$.*

Proof. By another homework problem, $\alpha \cap \beta \in \mathrm{On}$. If $\alpha \cap \beta = \alpha$ then $\alpha \subseteq \beta$ and $\alpha \leq \beta$. Similarly, if $\alpha \cap \beta = \beta$ then $\beta \leq \alpha$. If $\alpha \cap \beta \subsetneq \alpha, \beta$, then $\alpha \cap \beta \in \alpha, \beta$. Thus $\alpha \cap \beta \in \alpha \cap \beta$, which contradicts Foundation. $\square$

Theorem 5.5. *For every well-ordering (X, R) there exists a unique $\alpha \in \mathrm{On}$ such that $(X, R) \cong (\alpha, \in)$. This α is called the **order type** of (X, R).*

Proof. We fix X and R and claim that for every $\alpha \in X$, there exists a unique $\beta \in \mathrm{On}$ such that $I_a^R \cong (\beta, \in)$. Suppose not, and let a be a R-minimal counterexample. For every bRa, there exists a unique β_b such that $I_b^R \cong (\beta_b, \in)$. Then set $\beta = \{\beta_b : b \in \mathrm{pred}_R\, a\}$ is a set by replacement, and in fact, it is an ordinal. So we can take $\pi : I_a^R \to \beta$ by taking b to β_b. This is an order isomorphism.

So there always exists a unique $\beta_a \in \mathrm{On}$, and cal this map $a \mapsto \beta_a$. Then $\alpha = \{\beta_a : a \in X\}$ is an ordinal, and this map is a order morphism between α and X. $\square$

Theorem 5.6 (in ZF)**.** *The following are equivalent:*

(1) Well-ordering principle.

(2) For all X, Y, either $|X| \leq |Y|$ or $|Y| \leq |X|$.

Proof. For (1) $\Rightarrow$ (2), let X and Y be any sets and use well-ordering to get R, S. Use comparability to get $f : I_a^R \cong (Y, S)$ for some $a \in X$, or the other way round. Then $f^{-1} : Y \to X$ is an injection.

To do the other direction, we need the fact that ordinals can be larger than any set. Consider any X and get α with an injection $g : X \to \alpha$, by the next theorem. Set R on X by xRy if and only if $g(x) \in g(y)$. By injectivity, this is a well-order. $\square$

Theorem 5.7 (in ZF, Hartog)**.** *For every Y, there exists an α such that there is no injection from α into Y.*

Proof. Set

$$\alpha = \{\beta \in \mathrm{On} : \exists \text{injection} : \beta \to Y\}.$$

We need to verify that this is a set. First look at $\mathcal{P}(Y \times Y)$ which is a set, and let

$$A = \{R \in \mathcal{P}(Y \times Y) : R \text{ well orders some } Z \subseteq Y\}.$$

Then considering the map $A \ni R \mapsto \mathrm{ot}(\operatorname{dom} R, R)$. Then $\alpha \in \mathrm{On}$ is the image of this map.

By Foundation, $\alpha \notin \alpha$ and so there is no injection $\alpha \to Y$. We are done. $\square$

6 September 22, 2016

Lemma 6.1. *If $C \subset \mathrm{On}$ then $\bigcap C \in C$ and $\bigcap C$ is the minimal element of C.*

Proof. We first show that $\bigcap C$ is an ordinal. If $a \in b \in \bigcap C$ then for all $\gamma \in C$, we have $a \in b \in \gamma$ and so $a \in \gamma$ by transitivity. Then $a \in \gamma$ and so $a \in \bigcap C$. So $\bigcap C$ is transitive. Also $\bigcap C$ is linearly ordered under $\in$ as $\bigcap C$ is a subset of On.

Now let us prove that $\bigcap C \leq \gamma$ for all $\gamma \in C$. This is just because $\bigcap C \subset \gamma$ and so $\bigcap C \leq \gamma$.

Third, $\bigcap C$ is actually in C. Suppose $\bigcap C \notin C$. Then $\bigcap C < \gamma$ for all $\gamma \in C$. So $\bigcap C + 1 \leq \gamma$ for all $\gamma \in C$, and hence $\bigcap C + 1 \subseteq \bigcap C$. This is clearly a contradiction. $\square$

This shows that any subclass of On always has a minimal element. Note that this is not always true of linear orders, i.e., $\{a \in \mathbb{R} : a > \sqrt{2}\}$ does not have a minimal element.

6.1 Ordinal induction and arithmetic

Note all ordinals α fall into one of these three categories:

(1) $\alpha = 0$,

(2) α is a **successor**, i.e., $\alpha = \beta + 1$ for some β,

(3) α is a **limit**, i.e., there exists an increasing sequence $\langle \beta_i \rangle_{i \in \kappa}$ with $\beta_i < \alpha$ for all $i \in \kappa$ such that $\alpha = \bigcup_{i \in \kappa} \beta_i$.

Note that in the limit, the sequence cannot be indexed by the natural numbers. This is because the least ordinal not equinumerous with ω is not a countable union of smaller ordinals because all smaller ordinals will have at most ω many unions.

To prove that these cover all cases, let C be the class of ordinals that does not fall in these categories. Let α be the least element of C, which is $\alpha = \bigcup\{\beta : \beta < \alpha\}$, because α is not a successor.

Fix $\alpha \in \mathrm{On}$. We would like to define addition inductively. Define

(1) $\alpha + 0 = \alpha$,

(2) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$,

(3) if γ is a limit, then $\alpha + \gamma = \bigcup_{\beta < \gamma} \alpha + \beta$.

This can be visualized as just attaching β at the large end of α. This operation is *not* commutative, as $\omega + 2 \neq 2 + \omega = \omega$.

Likewise we define multiplication of the ordinals in the following way:

(1) $\alpha \cdot 0 = 0$,

(2) $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$,

(3) if γ is a limit ordinal then $\alpha \cdot \gamma = \bigcup_{\beta < \gamma} \alpha \cdot \beta$.

The way to look at it is to lay down α and copy that β times. For instance, $\omega \cdot 2 = (\omega \cdot 1) + \omega = \omega + \omega$. On the other hand, $2 \cdot \omega = \bigcup_{n<\omega} 2 \cdot n = \omega$. So multiplication is also not commutative.

Then we define exponentiation as

(1) $\alpha^0 = 1$,

(2) $\alpha^{\beta+1} = \alpha^\beta \cdot \beta$,

(3) if λ is a limit ordinal then $\alpha^\lambda = \bigcup_{\beta<\lambda} \alpha^\beta$.

Theorem 6.2. *Suppose $\beta > 0$. Then for all α there are unique α there are unique γ_1, γ_2 such that $\alpha = \beta \cdot \gamma_1 + \gamma_2$.*

Proof. First let us prove existence. Let $\gamma_1 = \bigcup\{\lambda : \beta \cdot \lambda \leq \alpha\}$. Then $\beta \cdot \gamma_1 \leq \alpha < \beta(\gamma_1 + 1)$. Once again, let $\gamma_2 = \bigcup\{\tau : \beta\gamma_1 + \tau \leq \alpha\}$. Then $\beta\gamma_1 + \gamma_2 \leq \alpha < \beta\gamma_1 + \gamma_2 + 1$.

To prove uniqueness, we first show that $\lambda < \tau$ then $\zeta + \lambda < \zeta + \tau$ for every ζ. This is true because we know that there exists a σ such that $\tau = \lambda + \sigma$ (by the existence part we have proved) and so $\zeta + \tau = \zeta + \lambda + \sigma > \zeta + \lambda$.

To show uniqueness, suppose that $\alpha = \beta\gamma_1^* + \gamma_2^*$ with $\gamma_2^* < \beta$. By the definition of γ_1, we have $\gamma_1^* \leq \gamma_1$ but if $\gamma_1^* < \gamma_1$ then $\beta(\gamma_1^* + 1) \leq \alpha$. Hence $\beta\gamma_1^* + \beta < \alpha$ which is a contradiction. So $\gamma_1^* = \gamma_1$. Similarly we get $\gamma_2^* = \gamma_2$. □

Theorem 6.3 (Cantor's normal form)**.** *Suppose $\alpha > 0$. Then α can be written uniquely as*

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$$

where $n \in \mathbb{N}$ and $\alpha \geq \beta_1 > \beta_2 > \cdots > \beta_n$ and all k_i are positive elements of $\mathbb{N}$.

Proof. Let us first show existence. If $\alpha = 1$, then it has a representation $\alpha = \omega^0 \cdot 1$. Now assume every $\alpha' < \alpha$ can be written in such a form. Let $\beta = \bigcup\{\beta' : \omega^{\beta'} \leq \alpha\}$. Then there are unique $\gamma_1, \gamma_2 < \omega^\beta$ such that $\alpha = \omega^\beta \cdot \gamma_1 + \gamma_2$ such that $\gamma_1 < \omega$ as otherwise $\omega^{\beta+1} \leq \alpha$. If $\gamma_2 = 0$, we are done. If $\gamma_2 > 9$ then $\gamma_2 < \omega^\beta < \alpha$ so γ_2 has the appropriate form. Then combining the representation with ω^β, we get the representation of β. □

One thing to note is that $\alpha \geq \beta_1$ contains equality. This is because ordinals ϵ such that $\epsilon = \omega^\epsilon$, which is quite different from cardinal arithmetic. Furthermore there even is an ordinal $\epsilon_0 = \epsilon_0^{\epsilon_0}$.

6.2 Building the universe

Definition 6.4. Define $V_0 = \emptyset$, $V_{\alpha+1} = \mathcal{P}(V_\alpha)$, and $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ if λ is a limit ordinal.

It turns out that these contain everything.

Lemma 6.5. $\{x : x = x\} = \bigcap_{\alpha \in \mathrm{On}} V_\alpha$.

Proof. It suffices to show that $x \subseteq \bigcap_{\alpha \in \mathrm{On}} V_\alpha$ then $x \in \bigcup_{\alpha \in \mathrm{On}} V_\alpha$. Note that by replacement, there exists a β such that $x \subseteq \bigcup_{\alpha<\beta} V_\alpha$. So $x \subseteq V_{\beta+\omega}$, so $x \in \mathcal{P}(V_{\beta+\omega}) = V_{\beta+\omega+1}$. $\square$

Definition 6.6. The **rank** of x is the least α such that $x \in V_\alpha$.

Theorem 6.7. *Assuming the axiom of choice, any set can be well-ordered.*

Proof. Let $f : \mathcal{P}(X) - \{\emptyset\} \to X$ be a choice function. Let h be defined by transfinite recursion using

$$h(\alpha) = f(X - \mathrm{range}(h|_\alpha))$$

when $\mathrm{range}(h|_\alpha) \neq X$. Let β be the least α such that $\mathrm{range}(h|_\alpha) = X$. Note as f is a choice function, h_β is a bijection. For $x, y \in X$, let xRy if $h^{-1}(x) < h^{-1}(y)$ then R well orders X. $\square$

6.3 Cardinals

Definition 6.8. We say that X and Y are **equinumerous** ($X \approx Y$) if there is a bijection from X to Y. We say $X \preccurlyeq Y$ if there is an injection from X into Y.

Theorem 6.9 (Cantor-Bernstein thereom)**.** *If $X \preccurlyeq Y$ and $Y \preccurlyeq X$ then $X \approx Y$.*

Proof. Suppose $f : X \to Y$ and $g : Y \to X$ are injections. Let $X_0 = X$ and $Y_0 = y$, and take $X_{n+1} = g''(Y_n)$ and $Y_{n+1} = f''(X_n)$. Let $X_\infty = \bigcap_{n\in\mathbb{N}} X_n$ and $Y_\infty = \bigcap_{n\in\mathbb{N}} Y_n$. Let

$$h(x) = \begin{cases} h(x) & \text{if } x \in X_{2n} - X_{2n+1} \\ g^{-1}(x) & \text{if } x \in X_{2n+1} - X_{2n+1} \\ f(x) & \text{if } x \in X_\infty. \end{cases}$$

Note that $f|_{X_{2n}-X_{2n+1} \to Y_{2n+1}-Y_{2n+2}}$ is a bijection, and $g^{-1}|_{X_{2n+1}-X_{2n+2} \to Y_{2n-1}-Y_{2n+1}}$ is a bijection. So h is a bijection when restricted to $X - X_\infty \to Y - Y_\infty$. Also h is an injection on X_∞ as f is an injection, and also it is surjection onto Y_∞. So $h : X \to Y$ is a bijection. $\square$

For example, we can easily show that $\mathbb{N} \approx \mathbb{Q}$. Clearly $\mathbb{N} \preccurlyeq \mathbb{Q}$ since $\mathbb{N} \subseteq \mathbb{Q}$. Next, we can set $r : \mathbb{Q} \to \mathbb{N}$ so that

$$r : (-1)^j \frac{a}{b} \mapsto 2^a 3^b 5^j$$

where $j \in \{0, 1\}$ and $\gcd(a, b)$. This is an injection, so $\mathbb{N} \approx \mathbb{Q}$.

Definition 6.10. We say that a real number x is **algebraic** if there exists $a_1, a_2, \ldots, a_n \in \mathbb{Q}$ such that $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. The set of algebraic numbers is denoted by $\mathbb{A}$.

Then $\mathbb{A} \approx \mathbb{N}$. Clearly $\mathbb{N} \preccurlyeq \mathbb{A}$, and by the injection $s : \mathbb{A} \to \mathbb{N}$

$$s(x) = 2^i 3^{r(a_0)} 5^{r(a_1)} 7^{r(a_2)} \cdots ,$$

where x is the ith solution of an irreducible $a_n x^n + \cdots + a_1 x + a_0 = 0$. So $\mathbb{A} \preccurlyeq \mathbb{N}$ and thus $A \approx \mathbb{N}$.

Definition 6.11. An ordinal α is a **cardinal** if $\beta \not\approx \alpha$ for every $\beta < \alpha$.

For instance, $\omega + \omega$ is not a cardinal. For each cardinal κ, let κ^+ be the least cardinal that is greater than κ.

7 September 27, 2016

Recall that α is an ordinal, then α is a cardinal if $\alpha \not\approx \beta$ for all $\beta < \alpha$. Also, κ is a cardinal, then κ^+ is the next cardinal. Finally, let Card be the collection or cardinals.

Lemma 7.1. *If $A \subseteq \text{Card}$ and A is a set, then $\bigcup A \in \text{Card}$.*

Proof. If A has a largest element κ, then $\bigcup A = \kappa \in \text{Card}$. Assume $\bigcup A \notin \text{Card}$ and A does not have a largest element to get a contradiction. There exists an $\alpha \in \bigcup A$ such that $\alpha \approx \bigcup A$. Let $\kappa \in A$ such that $\kappa < \alpha$. But then $\kappa \approx \alpha$ as $\alpha = |\bigcup A|$. □

Definition 7.2. Let $\aleph_0 = \omega$ and $\aleph_{\alpha+1} = \aleph_\alpha^+$ for all ordinals α, and let $\aleph_\lambda = \bigcup_{\alpha<\lambda} \aleph_\alpha$ for λ a limit.

Theorem 7.3. *If $\kappa \in \text{Card}$ then either κ is finite or $\kappa = \aleph_\alpha$ for some ordinal α.*

Proof. Let α be the least such that $\aleph_\alpha \geq \kappa$. If $\alpha = \beta + 1$ then $\aleph_\beta < \kappa$, so $\kappa = \aleph_\beta^+ = \aleph_\alpha$. If α is a limit then for all $\gamma < \alpha$, $\aleph_\gamma < \kappa$ so $\aleph_\alpha \leq \kappa$. So $\kappa = \aleph_\alpha$. □

Continuum Hypothesis (CH). *Every subset of $\mathcal{P}(\omega)$ that can not be mapped invectively into ω has a bijection with $\mathcal{P}(\omega)$.*

This was the first natural question arose that is independent of ZFC. Gödel's incompleteness theorem says that the consistency of Peano arithmetic is independent of Peano arithmetic, but this is kind of ad hoc.

7.1 Cardinal arithmetic

Generalized Continuum Hypothesis (GCH). *If κ is a cardinal then $\kappa^+ \approx \mathcal{P}(\kappa)$.*

Theorem 7.4. *GCH implies AC.*

Proof. Assume GCH. It suffices to show that for all α, $V_\alpha \approx \kappa$ for some cardinal κ. Assume not, and let α be the least one such that $V_\alpha \not\approx \kappa$ for any $\kappa \in \text{Card}$. Note that $\alpha \neq 0$. If α is a limit ordinal then for all $\gamma < \alpha$, V_γ is well-ordered. Let $\beth_\gamma$ be the cardinality of V_γ, and let $\beth_\alpha = \sup\{\beth_\gamma : \gamma < \alpha\}$. Note that $\beth_\alpha \cdot \alpha \approx \beth_\alpha$ because $\beth_\alpha \cdot \beth_\alpha = \beth_\alpha$. (We haven't prove this yet, but hopefully get to it.) So $\bigcup_{\gamma<\alpha} V_\gamma \leq \beth_\alpha \cdot \alpha$ and so $V_\alpha \leq \beth_\alpha$. But we know that $\beth_\gamma \leq V_\gamma$ for all $\gamma < \alpha$, and so

$$\bigcup_{\gamma<\alpha} \beth_\gamma \leq \bigcup V_\gamma \approx V_\alpha.$$

So $\beth_\alpha \approx V_\alpha$, which is a contradiction.

Now consider the case $\alpha = \beta + 1$. Then $V_\beta \approx \beth_\beta$ so by GCH, $\mathcal{P}(V_\beta) \approx V_{\beta+1} \approx \beth_\beta$. This is again a contradiction. □

Definition 7.5 (Assuming AC)**.** The **cardinality** of X, written as $|X|$, is the least ordinal α such that $X \approx \alpha$.

The reason we need AC is because we should know that X is equinumerous with at least one ordinal.

Definition 7.6. If $\kappa, \lambda \in \text{Card}$, then we define

$$\kappa + \lambda = |(\{0\} \times \kappa) \cup (\{1\} \times \lambda)|, \quad \kappa \cdot \lambda = |\kappa \times \lambda|.$$

Definition 7.7 (Assuming AC)**.** A set is **finite** if $|X| < \omega$, and a set is **infinite** if $|X| \geq \omega$.

Theorem 7.8. *If κ is an infinite cardinal then $\kappa \cdot \kappa = \kappa$.*

Proof. Base case $\omega \cdot \omega = \omega$ is straight forward. Assume this holds for all infinite $\alpha < \kappa$. We want to define a well-ordering on $\kappa \times \kappa$ of order type $(\kappa, \in)$. For $(\alpha, \beta), (\gamma, \delta) \in \kappa \times \kappa$, let

$$(\alpha, \beta) \lhd (\gamma, \delta) \quad \Leftrightarrow \quad \max(\alpha, \beta) < \max(\gamma, \delta) \text{ or } \max(\alpha, \beta) = \max(\gamma, \delta) \wedge (\alpha, \beta) <_{\text{lex}} (\gamma, \delta).$$

We claim (but not prove) that this is a well-ordering.

Note that for any $(\alpha, \beta) \in \kappa \times \kappa$,

$$|\{(\gamma, \delta) : (\gamma, \delta) \lhd (\alpha, \beta)\}| \leq |(\max(\alpha, \beta) + 1) \times (\max(\alpha, \beta) + 1)|.$$

But by the inductive hypothesis,

$$|(\max(\alpha, \beta) + 1) \times (\max(\alpha, \beta) + 1)| = |\max(\alpha, \beta) + 1| < \kappa.$$

So for $(\alpha, \beta) \in (\kappa, \kappa)$, (α, β) has at most κ many $\lhd$-predecessors. This shows that $(\kappa \times \kappa, \delta) \cong (\kappa, \in)$. $\square$

Corollary 7.9. *If $\kappa, \lambda \in$ Card and $\kappa, \lambda \neq 0$, and at least is infinite, then $\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}$.*

Definition 7.10 (Also under AC)**.** If $\kappa, \lambda \in \text{Card}$, let $\kappa^\lambda = |\{f : \lambda \to \kappa\}|$.

Lemma 7.11. *If A, B are sets then $A^B = \{f : A \to B\}$.*

Theorem 7.12. *For all sets A, B, C, $(A^B)^C \approx A^{B \times C}$.*

Proof. Fix $f \in (A^B)^C$, i.e., $f : C \to A^B$. For $c \in C$, let $f_c : B \to A$ be such that $f_c = f(c)$. Then define $f^* : B \times C \to A$ be such that $f^*(b, c) = f_c(b)$. It is easy to check that $f \mapsto f^*$ is a bijection. $\square$

Corollary 7.13 (Assuming AC)**.** *If $\kappa, \lambda, \mu \in$ Card, then $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$.*

Lemma 7.14. *If $2 \leq \kappa \leq \lambda$ and λ is infinite, then $2^\lambda = \kappa^\lambda$.*

Proof. This is because $2^\lambda \leq \kappa^\lambda \leq (2^\kappa)^\lambda = 2^{\kappa \cdot \lambda} = 2^\lambda$. $\square$

If $\lambda < \kappa$ then things are more interesting. Without AC, $X \approx Y$ is an equivalence relation.

What will happen if we don't have AC? Still $X \approx Y$ will be an equivalence relation, and $\{Y : X \approx Y\}$ will be a class. But there might not be a function $e : V \to V$ such that $e(X) \approx X$ for all X and $e(X) = e(Y)$ if and only if $X \approx Y$. There is a trick.

Scott's trick. *For all $X \in V$ consider the least α_X such that $\{Y : Y \approx X\} \cap V_{\alpha_X} \neq \emptyset$. We let $\{Y : Y \approx X\} \cap V_{\alpha_X}$ "represent" $|X|$.*

This works quite well as a representative.

7.2 Cofinality

Definition 7.15. Let α be a limit ordinal. The **cofinality** of α, $\mathrm{cof}(\alpha)$, is the least β such that there exists an $f : \beta \to \alpha$ such that for all $\bar{\alpha} < \alpha$ there exists an $\bar{\beta} < \beta$ such that $f(\bar{\beta}) > \bar{\alpha}$.

For example, $\mathrm{cof}(\aleph_\omega) = \omega$, because $f : n \mapsto \aleph_n$ is cofinal in $\aleph_\omega$.

Definition 7.16. A limit ordinal α is **regular** if $\mathrm{cof}(\alpha) = \alpha$. Otherwise, α is **singular**.

If κ is a limit and κ is regular, then $V_\kappa \models \mathrm{ZFC}$.

8 October 4, 2016

The countable union of countable sets is countable. This shows that I can't write $\aleph_1$ as a less than $\aleph_1$ sized union of less that $\aleph_1$ sized sets. For this reason, we are going to call $\aleph_1$ regular.

On the other hand, $\aleph_\omega = \sup_{n<\omega} \aleph_n$ and so $\aleph_\omega$ is the union of countably many less thab $\aleph_\omega$ sized sets. Then we are going to call $\aleph_\omega$ singular.

Definition 8.1. A function $f : \beta \to \alpha$ is **cofinal** if for every $\alpha' < \alpha$ there exists $\beta' < \beta$ such that $f(\beta') > \alpha'$. If α is a limit ordinal, the cofinality $\operatorname{cof}(\alpha)$ is $\operatorname{cof}(\alpha) = \min\{\beta : \exists \text{cofinal } f : \beta \to \alpha\}$.

Definition 8.2. A limit ordinal is **regular** if $\operatorname{cof}\alpha = \alpha$ and **singular** if $\operatorname{cof}\alpha < \alpha$. A limit ordinal α is **Godzilla** if $\operatorname{cof}\alpha > \alpha$.

Proposition 8.3. *There are no Godzilla ordinals.*

Proof. The map $\mathrm{id} : \alpha \to \alpha$ is cofinal. ☐

Lemma 8.4. *The composition of two increasing cofinal functions is cofinal.*

Lemma 8.5. *Let α be a limit ordinal. There is an increasing cofinal function $f : \operatorname{cof}\alpha \to \alpha$.*

Proof. Let $g : \operatorname{cof}\alpha \to \alpha$ be cofinal. Set $f(\beta) = \max\{g(\beta), \sup_{\gamma<\beta}(f(\gamma)+1)\}$. To define this function, we have to use transfinite recursion on $F : \operatorname{cof}\alpha \times V \to V$ given by

$$F(\beta, h) = \begin{cases} \max\{g(\beta), \sup_{\gamma<\beta}(h(\gamma)+1) & \text{if } h \text{ with } \beta \subseteq \operatorname{dom} h, \\ \{\{0\}\} & \text{otherwise.} \end{cases}$$

☐

The following all have cofinality ω:

$$\omega, \quad \aleph_\omega, \quad \omega+\omega, \quad \omega^2, \quad \kappa+\omega, \quad \aleph_{\omega^2}.$$

8.1 Successor cardinals are regular

Theorem 8.6. *For every cardinal κ, κ^+ is regular.*

Proposition 8.7. *If α is a limit ordinal,*

(1) $\operatorname{cof}(\operatorname{cof}(\alpha)) = \operatorname{cof}\alpha$.

(2) $\operatorname{cof}\alpha$ *is a regular cardinal.*

Proof. (1) Suppose $f : \operatorname{cof}\alpha \to \alpha$ and $g : \operatorname{cof}(\operatorname{cof}\alpha) \to \operatorname{cof}\alpha$ are increasing. Then their composite $f \circ g : \operatorname{cof}(\operatorname{cof}\alpha) \to \alpha$ is also cofinal, and since $\operatorname{cof}(\operatorname{cof}\alpha) \le \operatorname{cof}\alpha$, we are done by minimality.

(2) We need only prove that $\operatorname{cof}\alpha$ is a cardinal. If $\operatorname{cof}\alpha$ is not a cardinal, then there exists an $\gamma < \operatorname{cof}\alpha$ and a bijection $f : \gamma \to \operatorname{cof}\alpha$. Then we can compose f which is cofinal (or its modification that is both increasing and cofinal) and $\operatorname{cof}\alpha \to \alpha$ so that $\gamma \to \alpha$ is cofinal. This contradicts the minimality of $\operatorname{cof}\alpha$. ☐

Lemma 8.8. *If κ is a cardinal then κ is regular if and only if κ cannot be written as a $(< \kappa)$ sized union $(< \kappa)$ sized sets.*

Proof. Let us first prove the forward direction. For contradiction, suppose that κ is regular and $\kappa = \bigcup_{i<\alpha} X_i$ with $\alpha < \kappa$ and $|X_i| < \kappa$. Because κ is regular and $|X_i| < \kappa$, $\sup X_i < \kappa$ for each $i < \alpha$. Then the map $g : \alpha \to \kappa$ by $g(i) = \sup X_i$ is cofinal, because $\kappa = \bigcup_{i<\alpha} X_i$. This contradicts that κ is cofinal.

Let's now show the other direction. Suppose κ is singular and $\alpha = \operatorname{cof} \kappa < \kappa$. This means that there is a increasing cofinal function $f : \alpha \to \kappa$. Set $X_i = f(i) + 1$. Then $|X_i| < \kappa$ because $f(i) < \kappa$ and κ is a cardinal. Also $\bigcup_{i<\alpha} X_i = \kappa$ because given $\beta < \kappa$ there exists an $i < \alpha$ with $f(i) > \beta$. $\square$

Proof of Theorem 8.6. Suppose not. Then there exists a decomposition

$$\kappa = \bigcup_{i<\alpha} X_i$$

for $\alpha < \kappa^+$ and $|X_i| < \kappa^+$. Because only the cardinality of α matter, we may assume that $\alpha \leq \kappa$, and also $|X_i| \leq \kappa$. Then

$$\left|\bigcup_{i<\alpha} X_i\right| \leq \kappa \cdot \kappa = \kappa < \kappa^+.$$

This is a contradiction. And so κ^+ is regular. $\square$

9 October 4, 2016, Make-up class

9.1 Regular limit cardinals

Can limit cardinals be regular? I spoiled the answer by telling you that ZFC cannot decide.

Theorem 9.1. *If α is a limit ordinal, then* $\operatorname{cof} \aleph_\alpha = \operatorname{cof} \alpha$.

Lemma 9.2. *If $f : \beta \to \alpha$ is a function that is cofinal and nondecreasing, then* $\operatorname{cof} \beta = \operatorname{cof} \alpha$.

Proof. Let $g : \operatorname{cof} \alpha \to \alpha$ and $h : \operatorname{cof} \beta \to \beta$ be increasing and cofinal. Then $f \circ h : \operatorname{cof} \beta \to \alpha$ is cofinal, and this implies $\operatorname{cof} \alpha \leq \operatorname{cof} \beta$. For the other direction, define $k : \operatorname{cof} \alpha \to \beta$ by

$$k(\gamma) = \min\{\delta < \alpha : f(\delta) > g(\gamma)\}.$$

I want to show that k is cofinal. Let $\delta < \beta$. There exists and $\gamma' < \operatorname{cof} \alpha$ such that $g(\gamma') > f(\delta)$. Because $f(k(\gamma')) > g(\gamma') > f(\delta)$ and f is nondecreasing, $k(\gamma') > \delta$. Thus k is cofinal. So $\operatorname{cof} \beta \leq \operatorname{cof} \alpha$. $\square$

Proof of Theorem 9.1. The map $f : \alpha \to \aleph_\alpha$ given by $f(\beta) = \aleph_\beta$ is cofinal. Then by the lemma, $\operatorname{cof} \alpha = \operatorname{cof} \aleph_\alpha$. $\square$

Corollary 9.3. *There is no cofinal nondecreasing $f : \aleph_2 \to \aleph_1$.*

Corollary 9.4. *If $\alpha < \aleph_\alpha$, then $\aleph_\alpha$ is singular.*

Proof. $\operatorname{cof} \aleph_\alpha = \operatorname{cof} \alpha \leq \alpha < \aleph_\alpha$. $\square$

This proves that a lot of limit cardinals are singular. So the regular limit needs to satisfy $\alpha \geq \aleph_\alpha$.

Proposition 9.5. $\alpha \leq \aleph_\alpha$.

Proof. We use induction. Clearly $0 \leq \aleph_0$, and $\alpha \leq \aleph_\alpha$ implies $\alpha + 1 \leq \aleph_\alpha$. If α is a limit,

$$\alpha = \sup_{\beta<\alpha} \beta \leq \sup_{\beta<\alpha} \aleph_\beta = \aleph_\alpha. \qquad \square$$

There are indeed limit ordinals α with $\alpha = \aleph_\alpha$. Take $\alpha_0 = \omega$ and $\alpha_{n+1} = \aleph_{\alpha_n}$. Then we can set

$$\alpha_* = \sup_{n<\omega} \alpha_n.$$

This satisfy $\alpha_* = \aleph_{\alpha_*}$, because

$$\aleph_{\alpha_*} = \sup_{\beta<\alpha_*} \aleph_\beta = \sup_{n<\omega} \aleph_{\alpha_{n+1}} = \sup_{n<\omega} \alpha_{n+1} = \alpha_*.$$

So there are $\aleph$-fixed points. But the fixed point we have built has cofinality ω.

9.2 Inaccessible cardinals and models of ZFC

Definition 9.6. A cardinal κ is **weakly inaccessible** if it is a regular limit cardinal. κ is a **strong limit** if $\lambda < \kappa$ implies $2^\lambda < \kappa$. κ is **strongly inaccessible** if it is regular and strong limit.

Theorem 9.7 (König's theorem)**.** *For any cardinal κ, $\kappa^{\operatorname{cof}\kappa} > \kappa$. If $\lambda < \operatorname{cof}\kappa$ then $\kappa^\lambda = \sup_{\mu<\kappa} \mu^\lambda + \kappa$.*

Proof. (1) Let $f : \operatorname{cof}\kappa \to \kappa$ be cofinal and increasing. We know that $\kappa^{\operatorname{cof}\kappa} = |\operatorname{cof}\kappa \to \kappa|$. If $\kappa^{\operatorname{cof}\kappa} = \kappa$, let $\{g_\alpha : \alpha < \kappa\}$ enumerate $\operatorname{cof}\kappa \to \kappa$. Define $g : \operatorname{cof}\kappa \to \kappa$ by

$$g(\beta) = \min(\kappa - \{g_\alpha(\beta) : \alpha < f(\beta)\}).$$

Now I claim that for all $\alpha < \kappa$, $g_\alpha \neq g$. Find $\beta < \operatorname{cof}\kappa$ so that $f(\beta) > \alpha$. Then $g(\beta) \neq g_\alpha(\beta)$.

(2) Now suppose $\lambda < \operatorname{cof}\kappa$. Let $f : \lambda \to \kappa$. Then f can't be cofinal, so $\sup_{\alpha<\lambda} f(\alpha) < \kappa$. Set $\beta_f = \sup f``\lambda$. Then actually $f : \lambda \to \beta_f$. This shows that $\{\lambda \to \kappa\} = \bigcup_{\alpha<\kappa}\{\lambda \to \alpha\}$. Thus

$$\kappa^\lambda = |\lambda \to \kappa| = \Big|\bigcup_{\alpha<\kappa}\{\lambda \to \alpha\}\Big| \leq \sup_{\alpha<\kappa}|\lambda \to \alpha| = \sup_{\alpha<\kappa} \alpha^\lambda + \kappa. \qquad \square$$

We have a function $\aleph : \mathrm{On} \to \mathrm{Card}$ that is defined by

$$\aleph_\alpha = \begin{cases} \omega & \text{if } \alpha = 0 \\ \aleph_\beta^+ & \text{if } \alpha = \beta + 1 \\ \sup_{\beta<\alpha} \aleph_\alpha & \text{if } \alpha \text{ a limit.} \end{cases}$$

Now replacing the successor cardinal by taking exponentiation, we also get a function $\beth : \mathrm{On} \to \mathrm{Card}$ given by

$$\beth_\alpha = \begin{cases} \omega & \text{if } \alpha = 0 \\ 2^{\beth_\beta} & \text{if } \alpha = \beta + 1 \\ \sup_{\beta<\alpha} \beth_\alpha & \text{if } \alpha \text{ a limit.} \end{cases}$$

The continuum hypothesis then says that $\aleph_1 = \beth_1$, and the generalized continuum hypothesis states that $\aleph_\alpha = \beth_\alpha$ for all $\alpha \in \mathrm{On}$.

Recall that we have the hierarchy $V_0 = \emptyset$, $V_{\alpha+1}\mathcal{P}(V_\alpha)$, and $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$ for limit α. Then $V = \bigcup_{\alpha\in\mathrm{On}} V_\alpha$ is our universe. As we climb up, we would like to see how much of ZFC does the V_α satisfy.

What does it mean for V_α to satisfy an axiom of ZFC? We say that V_α satisfies an axiom φ if φ is true if we bind all quantifiers to V_α. For example, the Empty Set states that

$$\exists x, \forall y (y \notin x).$$

Now we restrict this to the set V_α and consider

$$\exists x \in V_\alpha, \forall y \in V_\alpha (y \notin x).$$

If $\alpha > 0$, this is going to be true since $\emptyset \in V_\alpha$.

Proposition 9.8. *For an ordinal α,*

(1) V_α satisfies Extensionality and Foundation.

(2) if $\alpha > 0$ then V_α satisfies Emptyset.

(3) if $\alpha > \omega$ then V_α satisfies Infinity.

(4) if α is limit then V_α satisfies Union, Pairing, and Powerset.

We need Replacement, which states that

$$\forall a, a_1, \ldots, a_n (\forall x \in a \exists! y\, \varphi(x, y, a_1, \ldots, a_n) \to \exists b \forall x \forall y \in b\, \varphi(x, y, a_1, \ldots, a_n)).$$

This is not always possible, because for instance the image of the function $n \in \omega \mapsto \omega + n$ does not give a set in $V_{\omega+\omega}$.

Now this problem arise because $\omega + \omega$ has small cofinality.

Theorem 9.9. *If κ is strongly inaccessible then V_κ satisfies Replacement.*

Proof. First note that $|V_{\omega+\alpha}| = \beta_\alpha$ by induction. Also, if κ is a $\beth$-fixed point because κ is strongly inaccessible.

Now suppose that $\varphi, a, a_1, \ldots, a_n \in V_k$ such that

$$\forall x \in a \exists! y \in V_k, \varphi(x, y, a_1, \ldots, a_n).$$

Then use replacement on φ^{V_k}, which is φ relativized to V_κ. This gives a $b \in V$ such that

$$\forall x \in a \exists! y \in b, \varphi(x, y, a_1, \ldots, a_n).$$

We then need to check that the image in b lives in V_κ.

We know that $a \in V_\kappa$, so $a \in V_{\omega+\alpha}$ for all $\alpha < \kappa$. Thus $|a| \leq |V_{\omega+\alpha}| = \beth_\alpha < \kappa$. Replacement gives a function $f : a \to b$ given by φ^{V_κ}. Now get a bijection $g : \lambda \to \alpha$ for some cardinal λ.

Define $h : \lambda \to \kappa$

$$h(\beta) = \operatorname{rank} f(g(\beta)).$$

Since $\lambda < \operatorname{cof} \kappa = \kappa$, h cannot be cofinal. So we get $\gamma = \sup_{\beta<\lambda} h(\beta) + 1$. Then $b \in V_{\gamma+1}$. This shows that V_κ satisfies Replacement. $\square$

Now we need to say why this shows that ZFC cannot prove nor disprove the existence of strongly inaccessible cardinals.

Theorem 9.10 (Gödel's Incompleteness Theorem)**.** *No sufficiently powerful consistence theory with a recursive axiomization can prove its consistency.*

Corollary 9.11. *ZFC cannot prove that ZFC is consistence.*

Corollary 9.12. *ZFC cannot prove the existence of a strongly inaccessible cardinal.*

Proof. Suppose it could. Then ZFC proves $\exists$ strongly inaccessible. But ZFC + $\exists$ strongly inaccessible proves V_κ satisfies ZFC. If a set satisfies some axioms, then they are consistent. So if ZFC proves existence of strongly inaccessible cardinals, then ZFC proves the consistency of ZFC. $\square$

We will see later that if ZFC proves the existence of weakly inaccessible cardinals, then ZFC proves the existence of strongly inaccessible cardinals.

10 October 6, 2016

So last lecture finishes introducing the basic notions. Now we are going to talk about problems we mentioned in first class.

10.1 The measure problem

Let's do a bit of introductory measure theory. We like $\mathbb{R}$ and would like to talk about the sizes of subsets of $\mathbb{R}$. One thing we can use is the cardinality of sets, but this is a very coarse notion.

Proposition 10.1. *For any $r < s$ in $\mathbb{R}$, $|(r, s)| = |\mathbb{R}|$.*

Proof. The function $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$ is a bijection. ☐

What about its length? We can define $\lambda((r, s)) = s - r$. Then problem with lengths is the this only works for intervals. This leads to the definition of a measure.

Definition 10.2. Given $\Gamma \subseteq \mathcal{P}(\mathbb{R})$, a **measure** $\mu : \Gamma \to \mathbb{R}_{\geq 0} \cup \{\infty\}$ is a function such that

(1) $\mu(\emptyset) = 0$, $\mu([0, 1]) = 1$,

(2) if $X, Y \in \Gamma$ and $X \subseteq Y$ then $\mu(X) \leq \mu(Y)$,

(3) if $X_n \in \Gamma$ for $n < \omega$ are pairwise disjoint, then

$$\mu\Big(\bigcup_{n<\omega} X_n\Big) = \sum_{n<\omega} \mu(X_n).$$

We say that μ is **translation invariant** if for all $X \in \Gamma$ and $r \in \mathbb{R}$, its translate $X + r \in \Gamma$ and $\mu(X) = \mu(X + r)$.

It follows from translation invariance and some other properties that $\mu((r, s)) = s - r$. Another good thing about translation invariance is that it excludes things like point measures.

For $X \subseteq \mathbb{R}$, define

$$\begin{aligned} \mu^*(X) &= \inf\{\textstyle\sum \ell(U_i) : U_i \text{ is an open cover of } X\}, \\ \mu_*(X) &= \sup_{\{} \textstyle\sum \ell(C_i) : C_i \text{ are closed and disjoint in } X\}. \end{aligned}$$

One is approximating X from the outside and one is approximating from the inside. Then X is called measurable if $\mu^*(X) = \mu_*(X)$.

Theorem 10.3 (Vitali)**.** *There is no translation measure on all of $\mathbb{R}$ (under AC).*

Proof. Set a relation $\sim$ on $\mathbb{R}$ by $r \sim s$ if $s - r \in \mathbb{Q}$. This is an equivalence relation. Now use the axiom of choice to pick one thing in each class in $[0, 1]$. This means a function $f : \mathbb{R}/\sim \to [0, 1]$ such that $f([r]_\sim) \sim r$. Now set

$$V = \{f([r]_\sim) : r \in \mathbb{R}\} \subseteq [0, 1].$$

Assume V is measurable by some μ. Set $Q = [-1, 1] \cap \mathbb{Q}$ and consider $\bigcup_{q \in Q'} V + q$. This satisfies

$$[0, 1] \subseteq \bigcup_{q \in Q'} V + q \subseteq [1, 2].$$

Also $V + q_0 \cap V + q_1 = \emptyset$. Then

$$1 \leq \sum_{n<\omega} \mu(V) \leq 3.$$

Now we have a problem. $\square$

Once you get to $\mathbb{R}^3$, things get a bit worse.

Theorem 10.4 (Banach-Tarski paradox)**.** *For $n \geq 3$, the unit ball in $\mathbb{R}^n$ can be decomposed into finitely many pieces and reassembled (by congruent actions) into two copies of itself.*

The problem is that the free group with 2 generators is non-amenable. For instance suppose there is a dictionary of all words using a and b. If you tear this into halves and erase all the first letters, you get two copies of the dictionary without doing anything too crazy. This is the key idea of the proof.

There are the open and closed sets, and there are also the Borel sets on the measurable sets. On the other hand, there are the Vitali sets and the set coming from the Banach-Tarski paradox on the complex and nonmeasurable side. So where is the line? This is what descriptive set theory is about.

10.2 The Baire space

Consider the **Baire space** ${}^\omega\omega$, which is the set of functions from ω to ω. There is a bijection $f : {}^\omega\omega \to \mathbb{R}$. But the real number has some more structure on it, and we need to keep some of this structure.

For $n < \omega$, the set ${}^n\omega$ is the functions from $n = \{0, \ldots, n-1\}$ to ω. All of these combined have a tree structure, by looking at the initial segments, which we denote by $\supseteq$. The Baire space lives over all of this.

Given two topological spaces X and Y, a map $f : X \to Y$ is a **homeomorphism** if and only if it is a bijection such that if $U \subseteq X$ is open then $f``U \subseteq Y$ is open, and if $V \subseteq Y$ is open then $f^{-1}V \subseteq X$ is open.

We will build a homeomorphism between ${}^\omega\omega$ and $\mathbb{R} - \mathbb{Q}$. This is good enough because $\mathbb{Q}$ has measure zero and nobody cares about $\mathbb{Q}$. To show this, we first need a topology on ${}^\omega\omega$.

Definition 10.5. For $s \in {}^{<\omega}\omega$, let $N_S = \{x \in {}^{\omega}\omega : S \subseteq X\}$.

Proposition 10.6. *The set* $\{N_s : s \in {}^{<\omega}\omega\}$ *forms a basis for the topology*

$$\tau = \{X \subseteq {}^{\omega}\omega : \forall x \in X \exists s \in {}^{<\omega}\omega \textit{ such that } x \in N_s \subseteq X\}.$$

Proof. We want to show that τ is a topology. Clearly $\emptyset, {}^{\omega}\omega \in \tau$ because $N_\emptyset = {}^{\omega}\omega$. It is also trivially closed under unions. Now let $X, Y \in \tau$ and $a \in X \cap Y$. Then there exists $s, t \in {}^{<\omega}\omega$ such that $a \in N_s \subseteq X$ and $a \in N_t \subseteq Y$. Then either $s \subseteq t$ or $t \subseteq s$. If $t \subseteq s$ then $a \in N_s = N_s \cap N_t \subseteq X \cap Y$. □

Proposition 10.7. *For all* $s \in {}^{<\omega}\omega$, N_s *is clopen.*

Proof. N_s is open by the definition of τ. Let $s \in {}^{n}\omega$. Then

$${}^{\omega}\omega - N_s = \{x \in {}^{\omega}\omega : s \not\subseteq x\} = \bigcup_{t \in {}^{n}\omega, t \neq s} N_t$$

is open. □

This shows that ${}^{\omega}\omega$ cannot be homeomorphic to $\mathbb{R}$.

Proposition 10.8. ${}^{\omega}\omega$ *is totally disconnected.*

Proof. Let $x \neq y \in {}^{\omega}\omega$. There exists a minimal $n < \omega$ such that

$$x \restriction n \neq y \restriction n = s \in {}^{n}\omega.$$

Then $y \in N_s$ and $x \in {}^{\omega}\omega - N_s$ will be a partition of ${}^{\omega}\omega$ into open sets. □

11 October 11, 2016

11.1 Midterm

There was a midterm. Here is an interesting question that appeared in the exam.

> The goal of this problem is to prove Mostowski's Collapsing Theorem using Transfinite Recursion.
>
> **Theorem 11.1** (Mostowski)**.** *If E is a well-founded and extensional relation on a set P, then there is a transitive set M and an isomorphism $\pi : (P, E) \cong (M, \in)$.*
>
> We say that a binary relation R on X is *extensional* iff for every $x, y \in X$, we have
>
> $$x = y \quad \Leftrightarrow \quad \forall z \in X (zRx \Leftrightarrow zRy).$$
>
> You can prove this theorem however you want, but here's a nice outline:
>
> (i) We wish to define π on P so that $\pi(x) = \{\pi(z) : zEx\}$. Find a function G so that the output of well-founded recursion is π (and show that this is the case).
>
> (ii) Show that π is injective and $xEy \Leftrightarrow \pi(x) \in \pi(y)$.
>
> (iii) Set $M = \pi"P$. Show that π is surjective and that M is transitive.
>
> (iv) Conclude the theorem.
>
> In fact this isomorphism is unique, but you don't need to show this. If you do show this, 5 bonus points.

12 October 18, 2016

Recall that the topology on ${}^\omega\omega$ is given by the clopen basis

$$N_s = \{x \in {}^\omega\omega : s \leq x\}$$

where $s = {}^{<\omega}\omega$.

12.1 Topology of ${}^\omega\omega$

Now we want to show that ${}^\omega\omega$ is homeomorphic to $(0,1) \setminus \mathbb{Q}$. The way we are going to do is to use continued fractions. Consider

$$\frac{26}{317} = \frac{1}{\frac{317}{26}} = \frac{1}{12 + \frac{5}{26}} = \frac{1}{12 + \frac{1}{5 + \frac{1}{5}}}.$$

Then we can associate to $26/317$ the sequence $[12, 5, 5]$.

Fix a $r \in (0,1)\setminus\mathbb{Q}$. Define the sequence $x_n^r \in (0,1)\setminus\mathbb{Q}$ and $k_n^r \in \omega_+ = \omega\setminus\{0\}$ for $n < \omega$ as

$$x_0^r = r, \quad k_0^r = \left\lfloor \frac{1}{x_0^r} \right\rfloor \quad \text{and} \quad x_{n+1}^r = \frac{1}{x_n^r} - k_n^r, \quad k_{n+1}^r = \left\lfloor \frac{1}{x_{n+1}^r} \right\rfloor.$$

This process never terminates because r is irrational. If this process never terminates, then r is in fact irrational because of the Euclidean algorithm. Then define

$$f : (0,1) \setminus \mathbb{Q} \to {}^\omega\omega_+; \quad f(r) = \langle k_0^r, k_1^r, \dots \rangle \in {}^\omega\omega.$$

Proposition 12.1. *The map f is a homeomorphism between $(0,1) \setminus \mathbb{Q}$ and ${}^\omega\omega$.*

To show this, we have to show that f is bijective, continuous, and its inverse is continuous.

We first show that f is injective. For contradiction, $r < s \in (0,1) \setminus \mathbb{Q}$ and $f(r) = f(s)$. We claim that if $r < t < s$, then $k_n^r = k_n^t = k_n^s$ and $(-1)^n x_n^r < (-1)^n x_n^t < (-1)^s x_n^s$. For $n = 0$, this is easy. Then

$$k_0^r = \left\lfloor \frac{1}{x_0^r} \right\rfloor \geq k_0^t = \left\lfloor \frac{1}{x_0^t} \right\rfloor \geq k_0^s \left\lfloor \frac{1}{x_0^s} \right\rfloor = k_0^r.$$

So $k_0^t = k_0^r = k_0^s = k_0$. The other parts can be worked out.

That f is surjective and continuous will be a homework.

So now let us prove that f^{-1} is continuous. Let $U \subseteq \mathbb{R}$ be an open set and we want to show that $f"U \subseteq {}^\omega\omega$ is open. In general, if $r < s \in (0,1) \setminus \mathbb{Q}$ and $l < \omega$ be the first index the expansions differ at. Then $r < s$ if and only if $(-1)^l (k_l^r - k_l^s) > 0$. This shows that

$$\frac{1}{k_0} > \frac{1}{k_0 + \frac{1}{k_1 + \frac{1}{k_2}}} > \cdots \text{ converges to } x \text{ from above,}$$

$$\frac{1}{k_0 + \frac{1}{k_1}} < \frac{1}{k_0 + \frac{1}{k_1 + \frac{1}{k_2 + \frac{1}{k_3}}}} < \cdots \text{ converges to } x \text{ from below.}$$

Going back to what we are trying to show, given $x \in U$ there exists an $\epsilon > 0$ such that $(x-\epsilon, x+\epsilon) \subseteq U$. Now find and N so that both sequences get in $(x-\epsilon, x+\epsilon)$. Letting $s = \langle k_0^x, k_1^x, \ldots, k_N^x \rangle \in {}^{<\omega}\omega$. Then you can show that $N_s \subseteq f"U$.

12.2 Measures on the Baire space

Knowing a measure on the irrationals would give us a measure on $\mathbb{R}$.

Proposition 12.2. *If $A \subseteq \mathbb{R}$ is countable, then A is Lebesgue measurable and $\mu(A) = 0$.*

Proof. Write $A = \{a_n : n < \omega\}$. If we prove that the outer measure is 0, then we are done. Take any $\epsilon > 0$, and look at

$$A \subseteq U_\epsilon = \bigcup_{n<\omega} \Big(a_n - \frac{1}{2^n}, a_n + \frac{1}{2^n}\Big).$$

Then $\mu^*(A) \leq \mu(U_\epsilon) = 4\epsilon$ for every $\epsilon > 0$. □

Corollary 12.3. $\mathbb{Q}$ *has measure* 0.

If λ is a measure on $\mathbb{R} \setminus \mathbb{Q}$, then $\lambda^+(A) = \lambda(A \setminus \mathbb{Q})$ is a measure on $\mathbb{R}$.

Now let us give a measure on ${}^\omega\omega$. Because ${}^\omega\omega = N_\emptyset$ corresponds to $(0,1)\setminus\mathbb{Q}$, we are going to make the measure of the whole space 1. Then for each finite sequence s, we have

$$N_s = N_{s\frown(0)} \cup N_{s\frown(1)} \cup N_{s\frown(2)} \cup \cdots.$$

We make each $N_{s\frown(k)}$ get a 2^{-k-1} proportion of N_s.

Definition 12.4. Let τ be the topology generated by $\mathcal{B} = \{N_s : s \in {}^{<\omega}\omega\}$. Define $\mu : B \to [0,1]$ by

$$\mu(N_s) = \prod_{i<n} \frac{1}{2^{s(i)+1}},$$

where $s \in {}^n\omega$.

13 October 20, 2016

We have defined the measure on the Baire space ${}^{\omega}\omega$.

13.1 Borel sets

We are going to define Borel sets by a hierarchy.

Definition 13.1. For $\alpha \in \mathrm{On}$ define $\Sigma^0_\alpha, \Pi^0_\alpha, \Delta^0_\alpha \subseteq \mathcal{P}({}^{\omega}\omega)$ in the following way. For $\alpha = 1$,

$$\Sigma^0_1 = \{\text{open sets}\}, \quad \Pi^0_1 = \{\text{closed sets}\}, \quad \Delta^0_1 = \Sigma^0_1 \cap \Pi^0_1 = \{\text{clopen sets}\}.$$

For $\alpha > 1$, we define

$$\Sigma^0_\alpha = \{A \subseteq {}^{\omega}\omega : A = \bigcup_{n<\omega} B_n \text{ for } B_n \in \bigcup_{\beta<\alpha} \Pi^0_\beta\},$$
$$\Pi^0_\alpha = \{A \subseteq {}^{\omega}\omega : {}^{\omega}\omega \setminus A \in \Sigma^0_\alpha\}, \quad \Delta^0_\sigma = \Pi^0_\alpha \cap \Sigma^0_\alpha.$$

We call $\Sigma^0_{\mathrm{On}} = \bigcup_{\alpha\in\mathrm{On}} \Sigma^0_\alpha$ the **Borel sets**.

Actually, you are going to see in your homework that $\Sigma^0_{\omega_1} = \Sigma^0_{\mathrm{On}}$. We also have this hierarchy:

$$\begin{tikzcd}[column sep=small, row sep=small]
 & \Sigma^0_1 \arrow[dr, phantom, sloped, "\subseteq"] & & \Sigma^0_2 \arrow[dr, phantom, sloped, "\subseteq"] & & \Sigma^0_3 \arrow[dr, phantom, sloped, "\subseteq"] & & & \\
\Delta^0_1 \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \Delta^0_2 \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \Delta^0_3 \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \Delta^0_4 \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \cdots \\
 & \Pi^0_1 \arrow[ur, phantom, sloped, "\subseteq"] & & \Pi^0_2 \arrow[ur, phantom, sloped, "\subseteq"] & & \Pi^0_3 \arrow[ur, phantom, sloped, "\subseteq"] & & &
\end{tikzcd}$$

This actually comes up in analysis. Σ^0_2 are the countable unions of closed sets, and Π^0_2 are the countable intersections of open sets.

Theorem 13.2. Σ^0_{On} *is the smallest* σ*-algebra containing closed the open sets and closed under complement and countable union.*

Proof. Let $A \in \Sigma^0_{\mathrm{On}}$. Then for some $\alpha \in \mathrm{On}$, $A \in \Sigma^0_\alpha$. For countable union, let $A_n \in \Sigma^0_{\mathrm{On}}$ for $n < \omega$. Let $\alpha_n \in \mathrm{On}$ such that $A_n \in \Sigma^0_\alpha$. Set $\beta = \bigcup_n \alpha_n$. Then $A_n \in \Sigma^0_\beta$ and so $A_n \in \Pi^0_{\beta+1}$. Thus $\bigcup_{n<\omega} A_n \in \Sigma^0_{\beta+2}$. This shows that Σ^0_{On} is closed under countable union and complement.

Now let us consider and arbitrary σ-algebra m. We show by induction that $\Sigma^0_\alpha \subseteq m$. For $\alpha = 1$, m contains the open sets, which is Σ^0_1. Let $\alpha > 1$ and suppose that $\Sigma^0_\beta \subseteq m$ for $\beta < \alpha$. Let $A \in \Sigma^0_\alpha$,r write $A = \bigcup_n B_n$ for $B_n \in \bigcup_\beta \Pi^0_\beta$. Then ${}^{\omega}\omega - B_n \in \bigcup_\beta \Sigma_\beta 0 \subseteq m$ and so

$$A = \bigcup_n ({}^{\omega}\omega \setminus ({}^{\omega}\omega \setminus B_n)) \in m.$$

This shows that $\Sigma^0_\alpha \subseteq m$. □

Then Borel sets are measurable, because measurable sets are closed under complement and countable unions. So Borel sets are on the measurable side.

13.2 Projective sets

I have told you the story of some graduate student worrying about the projection of a measurable set in $\mathbb{R}^2$ not being measurable. In fact, sets obtained by projection lie somewhere on the line between the measurable and the non-measurable side.

Consider the product $({}^\omega\omega)^n$. This space is the set of n-tuples of sequences of natural numbers, and the topology is given by the basis

$$\{N_{s_1} \times \cdots \times N_{s_n} : s_1, \ldots, s_n \in {}^\omega\omega\}.$$

Proposition 13.3. *The two spaces ${}^\omega\omega$ and $({}^\omega\omega)^n$ are homeomorphic.*

Proof. Fix some bijection $F : \omega \to {}^n\omega$. Define $G : {}^\omega\omega \to ({}^\omega\omega)^n$ by

$$G : x \in {}^\omega\omega \mapsto (\bar{x}_1, \ldots, \bar{x}_n) \quad \text{where} \quad \bar{x}_i(k) = F(x(k))(i). \qquad \square$$

This now gives us a measure, and Borel sets for $({}^\omega\omega)^n$. Now we are ready to define projective set.

Definition 13.4. Given $A \subseteq ({}^\omega\omega)^{n+m}$, define

$$\text{proj}_n(A) = \{x \in ({}^\omega\omega)^n : \exists y \in ({}^\omega\omega)^m \text{ such that } (x, y) \in A\}.$$

This is nice from a model theoretic point of view, because we can describe using a existential quantifier.

Definition 13.5. Define Σ^1_0 to be the Borel sets. We define

$$\begin{aligned}
\Sigma^1_1 &= \{A \subseteq ({}^\omega\omega)^n : A = \text{proj}_n(B) \text{ for Borel } B \subseteq ({}^\omega\omega)^{n+m}\}, \\
\Pi^1_1 &= \{\text{complements of elements of } \Sigma^1_1\}.
\end{aligned}$$

Then define similarly,

$$\begin{aligned}
\Sigma^1_{k+1} &= \{\text{proj}_n(A) : A \subseteq ({}^\omega\omega)^{m+n} \text{ is } \Pi^1_k\} \\
\Pi^1_{k+1} &= \{\text{complements of elements of } \Sigma^1_{k+1}\}.
\end{aligned}$$

Theorem 13.6 (Lusin)**.** *Σ^1_1 are measurable.*

The question is, are Σ^1_2 measurable? The amazing thing is that this is one of those maybe questions.

Theorem 13.7 (Solovay)**.** *If there exists an inaccessible cardinal, then then* Con(ZFC + *projective sets are measurable*)*.*

Theorem 13.8 (Shelah)**.** *If projective sets are measurable, then* Con(ZF + $\exists$*inaccessible cardinal*)*.*

There is somehow a connection between something that happens way above and something that happens on the ground.

13.3 Filters and ultrafilters

There is another approach to measure theory. Consider for example, the point measure, which is like $\mu_\varphi(A) = 1$ if $\varphi \in A$ and $\mu_\varphi(A) = 0$ if $\varphi \notin A$. This measure is $\{0,1\}$-valued, and we can represent μ_φ by a set $U_\varphi \subseteq \mathcal{P}(\mathbb{R})$ such that

$$A \in U_\varphi \quad \longleftrightarrow \quad \mu_\varphi(A) = 1.$$

This is exactly what a filter is.

Definition 13.9. Fix as set I. A set $F \subseteq \mathcal{P}(I)$ is a **filter** if

(a) $\emptyset \in F$, $I \notin F$.

(b) If $X \subset Y \subset I$ and $X \in F$, then $Y \in F$.

(c) If $X, Y \in F$, then $X \cap Y \in F$.

If F is a filter on I then μ_F on $\{A \subseteq I : A \in F \text{ or } I \setminus A \in F\}$ given by

$$\mu_F(A) = \begin{cases} 1 & \text{if } A \in F \\ 0 & \text{if not} \end{cases}$$

is a **finitely additive measure**.

Definition 13.10. A filter F on I is an **ultrafilter** if for every $X \subset I$, either $X \in F$ or $I \setminus X \in F$. A filter (or ultrafilter) F is **principal** if there exists an $x_0 \in I$ such that for all $A \subseteq I$, $A \in F$ implies $x_0 \in A$.

Every ultrafilter on a finite set is principal.

14 October 25, 2016

Recall that if we fix a set I, a **filter** F on I satisfies the axioms (1) $\emptyset \notin F$, $I \in F$, (2) $X \subseteq Y \subseteq I$ and $X \in F$ implies $Y \in F$, (3) $X, Y \in F$ implies $X \cap Y \in F$. A filter U is an **ultrafilter** if and only if for all $X \subseteq I$, either $X \in U$ or $I \setminus X \in U$.

Given a filter F, we can define a finitely additive measure μ_F on $\{X \subseteq I : X \in F \text{ or } I \setminus X \in F\}$.

Proposition 14.1. *A filter F is an ultrafilter if and only if it is maximal, i.e., if $F' \supseteq F$ is a filter then $F' = F$.*

Lemma 14.2. *If $F_0 \subseteq \mathcal{P}(I)$ satisfies for each $X_1, \ldots, X_n \in F_0$, $\bigcap_{i \leq n} X_i \neq$, then there is a filter $F \supseteq F_0$.*

Proof. Without loss of generality, assume $F_0 \neq \emptyset$. Define F by

$$F = \{X \subseteq I : \exists X_1, \ldots, X_n \in F_0 (\bigcap_{i \leq n} X_i \subseteq X)\}.$$

Then F is a filter. □

Proof of Proposition 14.1. I need to prove two directions. Suppose that F is an ultrafilter, and let $F' \supseteq F$. Assume that $X \in F'$ but $X \notin F$. Then $I \setminus X \in F$, and so $I \setminus X \in F'$. This contradicts that F' is a filter.

Now suppose F is a maximal filter. Let $X \subseteq I$. Then either $F_0 = F \cup \{X\}$ or $F_1 = F \cup \{I \setminus X\}$ has the finite intersection property. By the lemma and maximality of F, either $X \in F$ or $I \setminus X \in F$. This shows that F is an ultrafilter. □

14.1 Ultralimits

Theorem 14.3 (Bolzano-Weierstrass)**.** *Every bounded sequence has a convergent subsequence.*

This is a great theorem, but it is annoying that there are many limit points. So, is there a way of extending the "limit function" on convergent sequence to one on all sequences (with reasonable restrictions)? These restrictions will be stuff like, keeping sums and products, and the output should be a limit point.

Fix an ultrafilter U on ω. Define the **ultralimit** of $\langle a_n \in \mathbb{R} : n < \omega \rangle$ as

$$L = \lim_U a_n$$

if and only if for every $\epsilon > 0$ there exists an $X_\epsilon \in U$ such that for every $n \in X_\epsilon$, $|a_n - L| < \epsilon$.

Theorem 14.4. *Every bounded sequence has an ultralimit.*

Proof. Let $\langle a_n \rangle \subseteq [-B, B]$. Define by induction b_n, C_n, and $X_n \in U$ such that $b_n \leq b_{n+1} < c_{n+1} \leq c_n$ with $c_n - b_n \leq 2^{1-n} B$ and

$$X_n = \{k < \omega : a_k \in [b_n, c_n]\} \in U.$$

We construct the sequence by letting $b_0 = -B, c_0 = B$, $X_0 = \omega$, dividing the interval $[b_n, c_n]$ by half and choosing the large side. Let $L = \lim_{n\to\infty} b_n = \lim_{n\to\infty} c_n$. Then $L = \lim_U a_n$. $\square$

If U is a principal filter, which only cares only m, then $\lim_U a_n = a_m$.

14.2 Ultraproducts

Newton and Leibniz did calculus using infinitesimals, but they were not rigorous and were called "ghosts of departed quantities". Later Weierstrass and other people came up with the ϵ-δ definitions. But as ultrafilters were developed, Robbinson came up with a way of making it real math.

Fix a non-principal ultrafilter on ω. Set $\prod_{n<\omega} \mathbb{R} = {}^\omega\mathbb{R} = \{f : \omega \to \mathbb{R}\}$. But this is now not a field.

Definition 14.5. For $f, g \in \prod \mathbb{R}$, let $f =_U g$ if and only if $\{n < \omega : f(n) = g(n)\} \in U$.

Then this is an equivalence relation and respects $+$ and $=$. We say that $[f]_U < [g]_U$ if and only if $\{n \in w : f(n) < g(n)\} \in U$. The addition and multiplication behaves well under this order.

Definition 14.6. Define the **hyperreals** ${}^*\mathbb{R} = \prod \mathbb{R} / =_U$ with $+$, $\cdot$, $<$, etc.

You can define any function, like cos, on the hyperreals in a similar way.

Proposition 14.7. *The ring ${}^*\mathbb{R}$ has multiplicative inverses, i.e., is a field.*

15 October 25, 2016, Make-up class

15.1 Banach-Tarski Paradox

Let us first work in $\mathbb{R}^2$. Let C be the circle of radius 1 and let l be the line $(0,1)\times\{0\}$. Let ρ be the rotation of $\mathbb{R}$ about the origin by 1 rad. We know that $2\pi/1$ is irrational. Then for all $n \neq m$, $\rho^n(l)$ and $\rho^m(l)$ are disjoint. Let

$$A = C \cup \bigcup_{n=0}^{\infty} \rho^n(l).$$

Then $\rho(A) = C \cup \bigcup_{n=1}^{\infty} \rho^n(l)$ and so $A = \rho(A) \cup l$. This kind of thing is what we are going to do.

Denote by $\mathbb{F}_n$ the free group on n generators. The elements will be words made up of letters $x_1, \ldots, x_n$ and also $x_1^{-1}, \ldots, x_n^{-1}$, such that no x_i and x_i^{-1} are adjacent. Multiplication of two elements will be concatenating two words and canceling everything out.

Consider the free group $\mathbb{F}_2$ with generators x, y. Let $w(x)$ be the set of starting with x, and likewise define $w(y)$, $w(x^{-1})$, $w(y^{-1})$. Then there is a partition

$$\begin{aligned}
\mathbb{F}_2 &= \{e\} \cup w(x) \cup w(y) \cup w(x^{-1}) \cup w(y^{-1}) \\
&= x^{-1}w(x) \cup w(x^{-1}) \\
&= y^{-1}w(y) \cup w(y^{-1}).
\end{aligned}$$

Denote by SO_n the group of rotations of $\mathbb{R}^n$ about the origin, with multiplication being composition. Note that there is no embedding of $\mathbb{F}_2$ into SO_2. However, there is an embedding of $\mathbb{F}_2$ into SO_3, given by the generators that are the rotation φ about the x axis by $\arccos(1/3)$ and the rotation ψ about the z axis by $\arccos(1/3)$. Let $\langle \varphi, \psi \rangle$ be the subgroup of SO_3 generated by φ and ψ. The proof is a bunch of computation, but the point is that there is a copy of $\mathbb{F}_2$ in SO_3.

Let S^2 be the sphere of radius 1 in $\mathbb{R}^3$, and let B^3 be the closed ball of radius 1 in $\mathbb{R}^3$. Then the group $\langle \varphi, \psi \rangle$ acts on S^2 and gives gives an equivalence relation $p \sim q$ if and only if $\sigma(p) = q$ for some $\sigma \in \langle \varphi, \psi \rangle$.

We can try to set M^* to be the set of representatives. Then

$$S^2 = M^* \cup w(\varphi)M^* \cup w(\psi)M^* \cup w(\varphi^{-1})M^* \cup w(\psi^{-1})M^*$$

but it is not necessarily disjoint, because $1 \neq \sigma \in \langle \varphi, \psi \rangle$ may fix some stuff. So set

$$D = \{p \in S^2 : \exists 1 \neq \sigma \in \langle \varphi, \psi \rangle, \sigma(p) = p\}.$$

Then D is countable because $\mathbb{F}_2$ is countable and a rotation fixes exactly two points. Also $\langle \varphi, \psi \rangle (S^2 \setminus D) \subseteq (S^2 \setminus D)$.

So just as we had before, let $\sim$ be the equivalence relation on $S^2 \setminus D$ and let M be a set of representatives. Then

$$\begin{aligned} S^2 \setminus D = \langle \varphi, \psi \rangle M &= M \cup w(\varphi)M \cup w(\psi)M \cup w(\varphi^{-1})M \cup w(\psi^{-1})M \\ &= \varphi^{-1}w(\varphi)M \cup w(\varphi^{-1})M = \psi^{-1}w(\psi)M \cup w(\psi^{-1})M. \end{aligned}$$

are partitions.

How do we get rid of D? Since D is countable, we can find a rotation $\sigma \in \mathrm{SO}_3$ that fixes no element of D and sends no element of D to another under any iterations of σ. (First fixed the axis and then pick the angle.) Then for every $m \neq n$, $\sigma^m(D) \cap \sigma^n(D) \neq \emptyset$. If we set

$$D = \bigcup_{n<\omega} \sigma^n(D),$$

then $\sigma(E) = E \setminus D$. So you can rearrange $S^2 \setminus D$ to get S^2.

Now let us bring everything together. Note that "being able to decompose A into finitely many pieces an rearrange to make B by rigid motions" is an equivalence relation. We first make S^2 into $S^2 \setminus D$. Then using the fact that φ does not fix M, we make $S^2 \setminus D$ into $(S^2 \setminus D) \setminus M$. Using the decomposition

$$\langle \varphi, \psi \rangle = \varphi^{-1}w(\varphi) \cup w(\varphi^{-1}) = \psi^{-1}w(\psi) \cup w(\psi^{-1}),$$

we can make $(S^2 \setminus D) \setminus M$ into two pieces of $S^2 \setminus D$. Then we can track back and get to two pieces of S^2. Finally, we can extend this way of making two S^2s from S^2, to get a way of making two $B^3 \setminus \{0\}$ from one $B^3 \setminus \{0\}$. The way to fill this last center is to use the same thing: consider a circle passing through 0 and use an irrational rotation.

Theorem 15.1. *B^3 can be decomposed into finitely many pieces and then these pieces can be translated and rotated to get two copies of B^3.*

16 October 27, 2016

Last time we talked about the hyperreals, which is constructed by fixing an ultrafilter U on ω and putting an equivalence relation on $\prod \mathbb{R} = \{f : \omega \to \mathbb{R}\}$. Then we can extend functions $\mathbb{R} \to \mathbb{R}$ to ${}^*\mathbb{R} \to {}^*\mathbb{R}$.

Proposition 16.1. *For any $x \in {}^*\mathbb{R}$ with $x \neq 0$, there is an $y \in {}^*\mathbb{R}$ such that $xy = 1$.*

Proof. Then $\{n < \omega : f(n) \neq 0\} \in U$. Define

$$g(n) = \begin{cases} \frac{1}{f(n)} & f(n) \neq 0 \\ 0 & f(n) = 0. \end{cases}$$

Then $f \cdot g = 1$. □

This can be generalized.

Theorem 16.2 (Łoś)**.** *If $\varphi(x_1, \ldots, x_n)$ is any first order formula and $[f_1]_u, \ldots, [f_n]_u \in {}^*\mathbb{R}$, then $\varphi([f_1]_u, \ldots, [f_n]_u)$ holds if and only if $\{k < \omega : \varphi(f_1(k), \ldots, f_n(k))\}$ is in U.*

So $\mathbb{R}$ and ${}^*\mathbb{R}$ are exactly the same. But they are different, because the map $j : \mathbb{R} \to {}^*\mathbb{R}$ is injective but not surjective. For instance, $f(n) = n^{-1}$ is an infinitesimal that is greater than 0 but is smaller than any positive real number.

16.1 Dense linear orderings

Definition 16.3. A relation $(L, \leq)$ is a **dense linear ordering (without endpoints)** if

(1) $\leq$ is a linear ordering.

(2) For every $x < y \in L$ there exists a $z \in L$ such that $x < z < y$.

(3) For every $y \ni L$, there exist $x, z \in L$ such that $x < y < z$.

For example, $(\mathbb{Q}, <)$, $(\mathbb{R}, <)$, and $(\alpha \times \mathbb{Q}, <_{\text{lex}})$ are dense linear orderings.

Theorem 16.4 (Cantor's theorem)**.** *If $(L, \leq_L)$ is a countable dense linear ordering, then $(L, <_L) \cong (\mathbb{Q}, <)$.*

Proof. Write $L = \{a_n : n < \omega\}$ and $\mathbb{Q} = \{b_n : n < \omega\}$. Now we are going to do a "back and forth" definition. Build $\subseteq$-increasing functions f_n for $n < \omega$ such that

(a) $\operatorname{dom}(f_n) \subseteq L$ and $\operatorname{ran}(f_n) \subseteq \mathbb{Q}$,

(b) $\{a_1, \ldots, a_n\} \subseteq \operatorname{dom}(f_n)$ and $\{b_1, \ldots, b_n\} \subseteq \operatorname{ran}(f_n)$,

(c) $\operatorname{dom}(f_n)$ is finite,

(d) for every $x, y \in \operatorname{dom}(f_n)$, $x <_L y$ if and only if $f_n(x) < f_n(Y)$.

You can build this function by throwing in a_n or b_n in the function using that the orderings $<$ and $<_L$ are dense and without endpoints. Once you have this sequence, you can glue it as $f = \bigcup_{n<\omega} f_n$ to get an isomorphisms between $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$. $\square$

You can ask the same thing for $\mathbb{R}$. Is any dense linear ordering with the size $|\mathbb{R}|$ isomorphic to $\mathbb{R}$? There is set of the form $\alpha \times \mathbb{Q}$ that has the same cardinality with $\mathbb{R}$, and it is not isomorphic to $\mathbb{R}$.

Definition 16.5. A dense linear ordering $(L, <)$ is **separable** if and only if it has a countable dense subset. It is **complete** if and only if every $\emptyset \neq X \subsetneq L$ that is bounded above has a *least* upper bound.

Note that these are not first-order formulas because they involve the existence of sets.

Theorem 16.6. *If $(L, <)$ is a dense linear ordering without endpoints, separable and complete, then $(L, <_L) \cong (\mathbb{R}, <)$.*

Note that we are not requiring anything about the cardinality of L.

Proof. Let $X_0 \subseteq L$ be a dense countable subset. Then $(X_0, <)$ is a countable dense linear ordering without endpoints and so $(X_0, <) \cong (\mathbb{Q}, <)$. Define $f^* : L \to \mathbb{R}$ by

$$f^*(x) = \sup_{\mathbb{R}} \{f(y) : y \in X_0, y < x\}.$$

This is an isomorphism. $\square$

But mathematicians didn't stop here and wanted other characterizations.

Definition 16.7. A linear ordering $(L, <_L)$ satisfies the **countable chain condition** if and only if every collection of disjoint open intervals is countable.

Because every open set in $\mathbb{R}$ contains some rational number and $\mathbb{Q}$ is countable, $(\mathbb{R}, <)$ satisfies the countable chain condition. In general, if a dense linear ordering is separable, then it satisfies the countable chain condition.

Why is this called the countable chain condition? Given a partial order $(P, <)$, two elements $p, q \in P$ are called **incomparable** if $\neg(p \leq q \vee q \leq p)$. A set $C \subseteq P$ is an **antichain** if every $p \neq q \in C$ are incomparable, and we say that $C \subseteq P$ is a **strong (upward) antichain** if for every $x \neq y \in C$ there is no $z \in P$ such that $x <_P z$ and $y <_P z$. We say that P satisfies the κ-chain condition if and only if every strong antichain of P has size at most κ. In the case of the linear order $(L, <_L)$, we can form a partial order $(P, <_P)$ by letting $P = \{(a, b)_L : a < b \in L\}$ and $<_P$ is $\supseteq$. Then satisfying the countable chain conditions is equivalent to P satisfying the $\aleph_0$-chain condition.

Suslin's hypothesis. *Every complete dense linear ordering satisfying the countable chain condition is isomorphic to $\mathbb{R}$.*

A **Suslin line** is a complete dense linear ordering that does not satisfy the countable chain condition.

17 November 1, 2016

17.1 Trees

We kind of know trees. The set of finite sequences ${}^{<\omega}\omega$ has branches that keep branching. This is sort of the setup that we want to deal with. Note that there are no loops.

Definition 17.1. $(T, <_T)$ is a **partial order** if $<_T$ is a transitive binary relation. For an $x \in T$, define $\mathrm{pred}_{<_T}(x) = \{y \in T : y <_T x\}$. Then $\mathrm{pred}_{<_T}(x)$ is a partially ordered by the restriction of $<_T$.

Definition 17.2. A partial order $(T, <_T)$ is a **tree** if for every $x \in T$, $\mathrm{pred}_{<_T}(x)$ is well-ordered.

These trees can go infinitely wide, and also infinitely tall.

Definition 17.3. Let $(T, <_T)$ be a tree. For $x \in T$, define its **height** as $\mathrm{ht}_T(x)$ as the order type of $\mathrm{pred}_T(x)$. Define the **height** of T as $\mathrm{ht}_T = \sup\{\mathrm{ht}_T(x) + 1 : x \in T\}$. Also, for $\alpha < \mathrm{ht}_T$, the **α-level** of T is defined by

$$T_\alpha = \{x \in T : \mathrm{ht}_T(x) = \alpha\}.$$

For example, for ${}^{<\omega}\omega$, the n-level sets are the sequences of length n and $\mathrm{ht}_T = \omega$.

Example 17.4. Fix (infinite) cardinals κ, λ and set $T = ({}^{<\kappa}\lambda, \subseteq)$, which is the sequences in λ with length less than κ. This is a tree, that has height κ. Every tree is a subtree of this tree.

17.2 Branches of trees

Definition 17.5. A **branch** thorugh a tree $(T, <)$ is a sequence $b = \langle b_\alpha \in T : \alpha < \mathrm{ht}_T \rangle$ such that $b_\alpha \in T_\alpha$ and $\alpha < \beta$ implies $b_\alpha <_T b_\beta$.

Branches in ${}^{<\kappa}\lambda$ are given by $f \in {}^{\kappa}\lambda$.

Example 17.6. Let $T = (A, \subseteq)$ for $A \subseteq {}^{<\omega}\omega$ by

$$A = \{\langle n, n, \dots, n\rangle (k\text{-many}) : n < \omega, k \leq n\}.$$

This tree does not have any branches.

Definition 17.7. Say that a tree T is **$< \kappa$-branching** if every $x \in T$ has $< \kappa$ immediate successors. "Finitely branching" means "$< \omega$-branching".

Theorem 17.8 (König). *Any finitely splitting tree with a root of height ω has a branch.*

Proof. We are going to build $\langle s_n : n < \omega \rangle$ such that $S_n \in T_n$ and $s_n <_T s_{n+1}$ and $\{x \in T : s_n <_T x\}$ is infinite. Start with a root s_0. Then $\{x \in T : s_0 <_T x\} = T - \{s_0\}$ is infinite. Suppose we have s_n with immediate successors $t_1, \ldots, t_k$. Then

$$\operatorname{succ}(s_n) = \bigcup_{i=1}^{k} \operatorname{succ}(t_i) \cup \{t_1, \ldots, t_k\}.$$

So there exists an i_0 such that $\operatorname{succ}(t_{i_0})$ is infinite. $\square$

Definition 17.9. T is a **κ-tree** if $\mathrm{ht}_T = \kappa$ and T is $< \kappa$-splitting (and has $< \kappa$ many roots). This is the same as saying that for every $\alpha < \kappa$, $|T_\alpha| < \kappa$.

Note that there is a tree of height κ that is $< \kappa^+$-splitting and has no branch. To construct this, for $\alpha < \beta < \kappa$ define $s_{\alpha,\beta} \in {}^\alpha\kappa$ that is constant β. Then $T = \{s_{\alpha,\beta} : \alpha < \beta < \kappa\}$ is a tree with no branch. So we can restrict to κ-trees.

Likewise, if κ is singular, then there also exists a κ-tree with no branch. This is because you can construct the same tree but use the cofinal sequence instead of all of κ.

Anyways, all ω-trees always have branches, by König's theorem. We are going to prove next time that there is an ω_1-tree with no cofinal branches.

18 November 3, 2016

Recall that $(T, <_T)$ is a tree if for every $x \in T$, $\mathrm{pred}_{<T}(x)$ is well-ordered. A tree T is a κ-tree if and only if $\mathrm{ht}_T = \kappa$ and $|T_\alpha| < \kappa$ for every $\alpha < \kappa$.

18.1 ω_1-Aronszajn trees

Definition 18.1. T is called a **κ-Aronszajn tree** if it is a κ-tree with no cofinal branch.

So König's theorem says that there are no ω-Aronszajn trees. On the other hand there is an ω_1-Aronszajn tree.

Theorem 18.2 (Aronszajn)**.** *There is an ω_1-Aronszajn tree.*

Proof. As a first try, set

$$Q = \{s : \exists \alpha \in \mathrm{On} \text{ such that } s : \alpha \to \mathbb{Q} \text{ is increasing and } s \text{ has a maximum}\}.$$

Lemma 18.3. *If $\alpha < \omega_1$ then there exists an $A_\alpha \subseteq \mathbb{Q}$ such that* $\mathrm{ot}(A_\alpha, <) = \alpha$.

Because s has a max, either $\alpha = 0$ or $\alpha = \beta + 1$. Note that Q_n is the increasing sequences of length n for $n < \omega$. Then Q_ω is the increasing sequences of order type $\omega + 1$. For $\omega \leq \alpha < \omega_1$, Q_α is the increasing sequences of order type $\alpha + 1$.

We claim that $\mathrm{ht}_Q = \omega_1$. To show this, it suffices to show that for each $\alpha < \omega_1$, there exists an A_α such that $\mathrm{ot}_p(A_\alpha) = \alpha + 1$. This is true because there is an order preserving morphism from any countable ordinal to $\mathbb{Q}$. On the other hand, $\mathrm{ht}_Q \leq \omega_1$ because $\mathbb{Q}$ is countable.

This shows that Q has no cofinal branch. If there is one, then you can glue them to get a function on ω_1 to $\mathbb{Q}$. Are the levels of Q countable? This is not true because $Q_\omega \sim {}^{\omega+1}\mathbb{Q} \sim 2^{\aleph_0}$. So our first try doesn't really work.

Now build a subtree $T \subseteq Q$ with countable levels and $\mathrm{ht}_T = \omega_1$ but not changing the height notes. Define

$$(*)_\alpha = \left\{ \begin{array}{c} \forall \beta < \gamma < \alpha \text{ and } s \in T_\beta \text{ and } q \in \mathbb{Q} \text{ such that } \max s < q, \\ \exists t \in T_\gamma \text{ such that } s \subseteq t \text{ and } \max t < q \end{array} \right\}.$$

We are going to define T, and at the same time, prove that every level T_α satisfies $(*)_\alpha$. We define $T_0 = \emptyset$ and if T_α is defined and $(*)_{\alpha+1}$ holds,

$$T_{\alpha+1} = \{s \frown \langle q \rangle \in Q_{\alpha+1} : s \in T_\alpha, q \in \mathbb{Q}, q > \max(s)\}.$$

If α is a limit, then denote $T_{<\alpha} = \bigcup_{\beta<\alpha} T_\beta$. Because α is countable, $\mathrm{cof}(\alpha) = \omega$. Find an increasing sequence $\langle \alpha_n < \alpha : n < \omega \rangle$ such that $\sup_n \alpha_n = \alpha$. Let $x \in T_{<\alpha}$ and $q \in \mathbb{Q}$ such that $\max(s) < q$. Set $m = \min\{n : \alpha_n > \mathrm{ht}_T(x)\}$. Build an increasing sequence $\{x_n : n < \omega\}$ such that $x_0 = x$, $\mathrm{ht}_T\, x_n = \alpha_{m+n-1}$, and $\max(x_n) < q$, using $(*)$. Then set

$$y_{x,q} = \left(\bigcup_{n<\omega} x_n \right) \frown \langle q \rangle \in Q_\alpha.$$

Setting $T_\alpha = \{y_{x,q}\}$ works. $\square$

18.2 Other classes of tress

Definition 18.4. A tree is κ-**embeddable** if there exists a function $f : T \to \kappa$ such that $x <_T y$ implies $f(x) \neq f(y)$.

Definition 18.5. A tree is κ-**special** if it is the union of κ-many antichains.

Proposition 18.6. *If a κ^+-tree is κ-embeddable, then it has no cofinal branch.*

Proof. Restrict the function to a branch. □

Definition 18.7. A tree T is **normal** if $\kappa = \mathrm{ht}_T$ and

- $|T_0| = 1$,
- for every limit $\alpha < x$ and $x, y \in T_\alpha$, if $\mathrm{pred}_T(x) = \mathrm{pred}_T(y)$ then $x = y$,
- if $\alpha < \beta < \kappa$ and $x \in T_\alpha$ then there exists a $y \in T_\beta$ such that $x <_T y$,
- if $x \in T_\alpha$, then there exist $y_1, y_2 \in T_{\alpha+1}$ such that $x <_T y_1$ and $x <_T y_2$.

19 November 8, 2016

19.1 Suslin trees

Recall that $\mathbb{Q}$ is the countable dense linear ordering and $\mathbb{R}$ is the separable complete dense linear ordering. We asked if we can replace separability with the Suslin property, that every collection of disjoint open intervals is countable. A Suslin line is a complete dense linear ordering that is not separable.

Definition 19.1. A **Suslin tree** is an $\aleph_1$-Aronszajn tree that has no uncountable antichain.

Our goal is to prove that there exists a Suslin tree if and only if there exists a Suslin line.

Lemma 19.2. *If there is a Suslin tree, then there is a normal Suslin tree.*

We are again going to be doing some pruning.

Proof. Start with a Suslin tree T. We first make T have one root, by adding a common root. Then the new tree T^0 is still Suslin.

Suppose $x \in T^0$ cannot be arbitrarily extended, i.e., have a successor on all higher levels. Then $T^x = \{y \in T^0 : x <_0 y\}$ is countable. Let $T^1 = \{x \in T^0 : |T^x| > \omega\}$. This is a subset of T^0 so T^1 has no uncountable branches or antichains. Also $\mathrm{ht}_{T^1} = \omega_1$ because if $\mathrm{ht}_{T^1} = \beta < \omega_1$ then node in T_0 at level $\beta + 1$ has countably many successors and there are also countably many nodes below so T_0 is countable. This shows that T_1 is still Suslin. Also by a similar argument, every node is arbitrarily extendible.

Now we want to ensure every node has at least 2 immediate successors. We claim that if $\alpha < \omega_1$ and $x \in T^1_\alpha$, then there exists an $\beta > \alpha$ and $y_1 \neq y_2 \in T^1_\beta$ such that $x < y_1$ and $x < y_2$. This is because if such an x exists, then we can extend it to an branch by the arbitrary extendibility. Set $T^2 = \{x \in T^1 : x \text{ has } \geq 2 \text{ immediate successors}\}$ with the restricted orders. Again, it is clear that T^2 has no uncountable branches and antichains. Because level sets are antichains, this includes the fact that level sets are countable. Then everything works out fine and because splitting occurs cofinally, T^2 is Suslin.

Finally we need to take care of the splitting at limit levels. In the case that two or more nodes at a limit level have same predecessors, add a node there right below the limit level and make T^3. This additional node will take care of the problem. Finally, T^3 is a normal Suslin tree. □

Theorem 19.3. *There is a Suslin tree if and only if there is a Suslin line.*

Proof. First consider a Suslin line L. Because it is not separable, no countable $L_0 \subseteq L$ is dense. Note that disjoint unions corresponded to strong (upward) antichains. We are going to build intervals $\{I_\alpha = (a_\alpha, b_\alpha) : \alpha < \omega_1\}$ so that $(\{I_\alpha\}, \supseteq)$ is a Suslin tree. Let I_0 be an arbitrary interval. For $\alpha > 0$, the set $C = \{a_\beta, b_\beta : \beta < \alpha\}$ is countable. Find $I_\alpha = (a_\alpha, b_\alpha)_L$ whose closure is disjoint from C. Then for $\beta < \alpha$, either $I_\beta \cap I_\alpha = \emptyset$ or $I_\alpha \subsetneq I_\beta$. Then $\{I_\alpha\}$ form an tree under $\supseteq$ because every subset has a $\supseteq$-minimal element. It has no ω_1-sized antichain because L satisfies the Suslin property. Also its height is at most ω_1 but it has ω_1 elements, so its height is exactly ω_1. Finally, there is no branch because a branch will give rise to a ω_1-many collection of disjoint open intervals. So T is a Suslin tree.

Now consider a normal Suslin tree T. We may assume that for $x \in T$, $\operatorname{succ}(x) = \{y \in T_{\operatorname{ht}_T(x)+1} : x <_T y\}$ is countably infinite. For each x, let $<^x$ be a linear order on $\operatorname{succ}(x)$ so that $\operatorname{succ}(x) \cong \mathbb{Q}$. Order T by $<_*$, that is defined as,

$$x <_* y \ \Leftrightarrow \ x < y \text{ or } \begin{Bmatrix} z \in T = \max(\operatorname{pred} x \cap \operatorname{pred} y) \text{ and} \\ x' \neq y' \in \operatorname{succ}(z), x' < x, y' < y \text{ and } x' <^z y'. \end{Bmatrix}$$

Then $(T, <_*)$ is a dense linear ordering. If X is a collection of disjoint intervals in $(T, <_*)$, then we can pick $a_I \in I$ for each $I \in X$ to get an antichain $\{a_I\}_{I \in X}$ in T. Finally, if $D \subseteq T$ is countable, then $\alpha = \sup\{\operatorname{ht}_T x : x \in D\} < \omega_1$ and so we can pick to stuff above level α. This shows that this is a Suslin line. $\square$

20 November 10, 2016

What does it mean for something to be independent of something? A statement φ is **independent** of axioms T if and only if there is a model T satisfying φ and a model T failing φ.

Example 20.1. "Being abelian" is independent of the group axioms. This simply means that you can't neither prove nor disprove "being abelian" from just the group axioms. On the other hand, "product of two elements have an inverse" is not independent from the group axioms.

We've been saying that $2^{\aleph_0} = \aleph_1$ is independent from ZFC. To prove this, we have to construct two models of ZFC, one that satisfies the continuum hypothesis and one that fails the continuum hypothesis. But how do we build models? We already have V as a model, but we don't know anything else. We can try to find a model $M \subseteq V$, that satisfies ZFC. Or we can try to find $V \subseteq M$ outside V. For instance, if κ is a strongly inaccessible cardinal, then V_κ is a model of ZFC. We are soon going to construct L that has the same ordinals as in V.

There are two metamathematical perspectives we can take. We can use V only as our universe/starting model of ZFC. But then we run into class/definablity issues. The other way is to start with some set V' that is a model of ZFC and treat V' as V. But then we have to assume Con(ZFC) and is also less satisfying because all we are talking about is not all of math but a small chunk of math that is indistinguishable from all of math from the inside. We are mainly going to work in the second viewpoint.

20.1 The idea of L

Recall that we have defined $V_0 = \emptyset$, $V_{\alpha+1} = \mathcal{P}(V_\alpha)$, and $V_\delta = \bigcup_{\alpha<\delta} V_\alpha$ if δ is a limit. Then $V = \bigcup_{\alpha \in \mathrm{On}} V_\alpha$. But if we need only to get a model of ZFC, we don't really need to include everything at each step. Define

$$\mathrm{Def}(X) = \left\{ A \subseteq X : \begin{array}{c} \exists \text{ first-order formula } \varphi(x, y_1, \dots, y_n) \text{ and } a_1, \dots, a_n \in X \\ \text{such that } A = \{x \in X : \varphi(x, a_1, \dots, a_n)\} \end{array} \right\}.$$

If M satisfies ZFC and $X \in M$, then we expect $\mathrm{Def}(X) \subseteq M$.

Now if this is true, we are going to define L as

$$L_0 = \emptyset, \quad L_{\alpha+1} = \mathrm{Def}(L_\alpha), \quad L_\delta = \bigcup_{\alpha<\delta} L_\alpha \text{ for limit } \delta, \quad L = \bigcup_{\alpha \in \mathrm{On}} L_\alpha.$$

Doing this is much subtle than just constructing abelian groups and non-abelian groups, because this L is going to be our new "universe" and there are metamathematical issues. So we need to be really precise in working with these.

20.2 First-order logic

Logic starts with a language (that always have =). A **language** L consists of

- function symbols F with some arity $n_F < \omega$ (i.e., binary, ternary, n-ary, etc.),
- relations symbols R with some arity $n_R < \omega$,
- constant symbols c.

We also need some syntax that tells us how to construct sentences and semantics that tells us how sentences connect to the real world.

Let us describe the **syntax** of L. We define the **terms** $\mathrm{Terms}(L)$ as the smallest set containing

(1) every constant c of L,
(2) every variable x (from a fixed infinite set),
(3) if $t_1, \ldots, t_n \in \mathrm{Terms}(L)$ and $F \in L$ is an n-ary function, then $F(t_1, \ldots, t_n)$.

For instance, in the language of rings, the terms are things that can be made by multiplying and adding variables.

The **formulas** $\mathrm{Formulas}(L)$ is the smallest set containing

(1) if $t_1, \ldots, t_n \in \mathrm{Terms}(L)$ and $R \in L$ is an n-ary relation, then $R(t_1, \ldots, t_n)$,
(2) if $\varphi, \psi \in \mathrm{Formulas}(L)$, then $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$,
(3) if $\varphi \in \mathrm{Formulas}(L)$ and x is a variable, then $\exists x\varphi$ and $\forall x\varphi$.

In relation to set theory, in the language of set theory, $L = \{\in, =\}$ and $\mathrm{Terms}(L) = \{x : x \text{ is a variable}\}$. So far, we don't know how to interpret these sentences. But before this, we need to make sure we are not trying to interpret sentences like $\forall y(\neg y \in x)$.

Define the **free variable** function FV inductively. For terms, we set

$$\mathrm{FV}(c) = \emptyset, \quad \mathrm{FV}(x) = \{x\}, \quad \mathrm{FV}(F(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} \mathrm{FV}(t_i).$$

Then for formulas, we let

$$\mathrm{FV}(R(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} \mathrm{FV}(t_i), \quad \mathrm{FV}(\neg\varphi) = \mathrm{FV}(\varphi),$$
$$\mathrm{FV}(\varphi \wedge \psi) = \mathrm{FV}(\varphi) \cup \mathrm{FV}(\psi), \quad \mathrm{FV}(\exists x\varphi) = \mathrm{FV}(\varphi) \setminus \{x\}.$$

Write $\varphi(x_1, \ldots, x_n)$ to mean $\varphi \in \mathrm{Formulas}(L)$ and $FV(\varphi) \subseteq \{x_1, \ldots, x_n\}$. In short:

Terms:	combine constants, variables, and functions.
Atomic formulas:	relations between terms.
Formulas:	closure of atomic formulas under logical operations.

Now let us get to semantics. Fix a language L. An L-structure or L-model M consists of

- a universe/underlying set $|M|$,
- for $F \in L$ with arity n, a map $F^M : M^n \to M$,
- for n-ary relation $R \in L$, $R^M \subseteq M^n$,
- for constant $c \in L$, an element $c^M \in L$.

If we have a term t and an L-structure M with $\mathrm{FV}(t) = \{x_1, \ldots, x_n\}$, build $t^M : M^n \to M$ as follows:

- $(c)^M : M^0 \to M$ has value c^M,
- $x^M : M \to M$ is the identity,
- $F(t_1, \ldots, F_n) : M^n \to M$ is $(m_1, \ldots, m_n) \mapsto F^M(t_1(m_\bullet), \ldots, t_m(m_\bullet))$.

For $\varphi(x_1, \ldots, x_n) \in \text{Formulas}(L)$, M an L-structure, and $a_1, \ldots, a_n \in M$, we are going to define $M \vDash \varphi(a_1, \ldots, a_n)$ again inductively as:

- if $\varphi = R(t_1(x_\bullet), \ldots, t_m(x_\bullet))$, then
$$(M \vDash \varphi(a_1, \ldots, a_n)) = ((t_1^M(a_\bullet), \ldots, t_m^M(a_\bullet)) \in R^M).$$
- if $\varphi = \neg\psi$, then
$$(M \vDash \varphi(a_1, \ldots, a_n)) = \neg(M \vDash \psi(a_1, \ldots, a_n)).$$
- if $\varphi = \psi_1 \wedge \psi_2$, then
$$(M \vDash \varphi(a_1, \ldots, a_n)) = (M \vDash \psi(a_1, \ldots, a_n)) \wedge (M \vDash \psi(a_1, \ldots, a_n)).$$
- if $v\varphi(x_1, \ldots, x_n) = \exists y \psi(y, x_1, \ldots, x_n)$, then
$$(M \vDash \varphi(a_1, \ldots, a_n)) = \exists b \in M, (M \vDash \psi(b, a_1, \ldots, a_n)).$$

Note that you are only able to quantify over elements. So in the language of graphs, the notion of being connected can't naturally be described in first logic, because it is "there exists a $n < \omega$ and vertices $x_0, \ldots, x_n$ such that $x_0 = x$ and $x_n = y$ and $(x_i, x_{i+1}) \in E$". You can't quantify over a varying number of variables.

21 November 15, 2016

Last time we set up the notion of first-order logic. For set theory, the language is $\tau = \{E\}$. The syntax is built from xEy nd logical operations like negation, conjunction, and quantification. On the semantic side, there is a structure $\mathcal{M} = (M, E^{\mathcal{M}})$ consisting of a set M and $E^{\mathcal{M}} \subseteq M^2$. Finally, we have semantics, that is, given an $\varphi(x_1, \dots, x_n)$ and $a_1, \dots, a_n$, $\mathcal{M} \vDash \varphi(a_1, \dots, a_n)$.

21.1 Substructures and elementary substructures

Given τ-structures $\mathcal{M}$ and $\mathcal{N}$, we say that $\mathcal{M} \subseteq \mathcal{N}$ ($\mathcal{M}$ is a **substructure** of $\mathcal{N}$) if

- $M \subseteq N$, and
- for every n-ary $F \in \tau$, $F^{\mathcal{N}} \upharpoonright M^n = F^{\mathcal{M}}$,
- for every n-ary $R \in \tau$, $R^{\mathcal{N}} \cap M^n = R^{\mathcal{M}}$,
- for every $c \in \tau$, $c^{\mathcal{N}} = c^{\mathcal{M}}$.

This comes up in every parts of mathematics. But by what we have done so far, we have a tighter connection between the two structures.

Now this substructure axioms implies that $\mathcal{M} \vDash aEb$ if and only if $\mathcal{N} \vDash aEb$ for every $a, b \in M$. Given τ-structures $\mathcal{M}$ and $\mathcal{N}$, we say $\mathcal{M} \preccurlyeq \mathcal{N}$ ($\mathcal{M}$ is an **elementary substructure** of $\mathcal{N}$) if and only if

(a) $\mathcal{M} \subseteq \mathcal{N}$,

(b) if $\varphi(x_1, \dots, x_n)$ is a formula and $a_1, \dots, a_n \in M$, then

$$\mathcal{M} \vDash \varphi(a_1, \dots, a_n) \text{ if and only if } \mathcal{N} \vDash \varphi(a_1, \dots, a_n).$$

Let us look at an example. Take $\tau = \{<\}$ and $\mathcal{M} = (\omega \setminus \{0\}, \in)$ and $\mathcal{N} = (\omega, \in)$. Then $\mathcal{M} \subseteq \mathcal{N}$, but $\mathcal{M} \not\preccurlyeq \mathcal{N}$. This is because if we let $\varphi(y) = \forall x(x = y \vee y < x)$ then

$$\mathcal{M} \vDash \varphi(1) \quad \text{but} \quad \mathcal{N} \nvDash \varphi(1).$$

However, $\mathcal{M} \cong \mathcal{N}$ with the isomorphism given by $M \ni x \mapsto x - 1 \in N$. Here, two structures are called isomorphic if there exists an $f : M \to N$ such that

- f is a bijection,
- if $F \in \tau$ and $a_1, \dots, a_n \in F$, then $f(F^{\mathcal{M}}(a_1, \dots, a_n)) = F^n(f(a_1, \dots, a_n))$,
- if $R \in \tau$ and $a_1, \dots, a_n \in M$, then $(a_1, \dots, a_n) \in R^{\mathcal{M}}$ if and only if $(f(a_1), \dots, f(a_n)) \in R^{\mathcal{N}}$,
- if $c \in \tau$, then $f(c^{\mathcal{M}}) = c^{\mathcal{N}}$.

Proposition 21.1. *Let $\mathcal{M}$, $\mathcal{N}$ be $\{E\}$-structures and let $\mathcal{M} \preccurlyeq \mathcal{N}$. If $\mathcal{M}$ is a model of* ZFC*, so is $\mathcal{N}$.*

Proof. For each sentence φ in ZFC, $M \vDash \varphi$ if and only if $N \vDash \varphi$ by definition of $\preccurlyeq$. $\square$

Theorem 21.2 (Downward Löwenheim–Skolem–Tarski theorem). *Given a τ-structure $\mathcal{M}$ and $A \subseteq M$, there is a τ-structure $\mathcal{N}$ such that*

(1) $\mathcal{N} \preccurlyeq \mathcal{M}$,

(2) $A \subseteq N$,

(3) $|N| \leq |\tau| + |A| + \aleph_0$.

Proof. This is going to be a homework. $\square$

21.2 Models of set theory

From now on, we are going to focus on $\tau = \{E\}$ and typically M will satisfy some fragment of ZFC. Recall that X is transitive if $z \in y \in X$ implies $z \in X$. We also want to focus on structures $\mathcal{M}$ where M is transitive and $E^{\mathcal{M}} = \in$ (restricted to M).

We might have this weird situation where $\mathcal{M}$ satisfies the well-foundedness axiom but there are infinite decreasing $E^{\mathcal{M}}$-chains. Start with a structure $\mathcal{N} = (N, E)$ that satisfies ZFC. Take a non-principal ultrafilter U on ω, and form the ultraproduct $\mathcal{N}^* = \prod(N, E)/U$ so that $N^* = \{[f]_U : (f : \omega \to U)\}$ and

$$[f]_U E^* [g]_U \quad \Leftrightarrow \quad \{n < \omega : \mathcal{N} \vDash f(n) E g(n)\} \in U.$$

It turns out that $\mathcal{N}^*$ also satisfies ZFC including well-foundedness. But for $k < \omega$, we get take

$$f_k : n \mapsto \begin{cases} 0 & \text{if } n \leq k \\ n - k & \text{if } n > k \end{cases}$$

and this is a infinite decreasing sequence, i.e., $\mathcal{N}^* \vDash [f_{k+1}]_U E [f_k]_U$. This is why we want transitivity.

Theorem 21.3 (Mostowski). *Suppose $\mathcal{M}$ is a $\{E\}$-structure that satisfies extensionality and such that $E^{\mathcal{M}}$ is well-founded (actually well-founded, not satisfies the axiom). Then there is a unique transitive set X and an isomorphism $\pi : \mathcal{M} \cong (X, \in)$.*

This theorem allows us to check axioms more easily.

21.3 Lévy hierarchy

There is also the Lévy hierarchy that allows to rank the complexity of formulas. Of course you can define the complexity as the number of quantifiers, but there are certain **bounded quantifier** that is of the form

$$\exists x \in y \varphi(x, y, z_1, \ldots, x_n) \quad \text{or} \quad \forall x \in y \varphi(x, y, z_1, \ldots, z_n).$$

If $\mathcal{M} \subseteq \mathcal{N}$ but $\mathcal{M} \not\preccurlyeq \mathcal{N}$, then the failure must start at some quantification. But this first failure cannot happen at a bounded quantifier because if $y \in M$ then automatically $x \in M$.

Let us know define the **Lévy hierarchy**. We let

$$\Delta_0 = \Sigma_0 = \Pi_0$$

as formulas with just bounded quantification. So this is the minimal set such that when we quantify, $\varphi(x, y, z_1, \dots, z_n) \in \Delta_0$, then $\exists x \in y \varphi(x, y, z_1, \dots, z_n) \in \Delta_0$. We then let $\varphi(y_1, \dots, y_n) \in \Sigma_{k+1}$ if it is

$$\exists x_1 \cdots \exists x_l \psi(x_1, \dots, x_l, y_1, \dots, y_n).$$

We say that $\varphi \in \Pi_{k+1}$ if it is

$$\forall x_1 \cdots \forall x_l \psi(x_1, \dots, x_l, y_1, \dots, y_n).$$

We finally define $\Delta_{k+1} = \Sigma_{k+1} \cap \Pi_{k+1}$. Here, we are looking at equivalence classes of formulas.

Proposition 21.4. *If $\varphi(x_1, \dots, x_n)$ is Δ_0 and $\mathcal{M} \subseteq \mathcal{N}$ have transitive underlying sets, then for all $a_1, \dots, a_n \in M$, $\mathcal{M} \vDash \varphi(a_1, \dots, a_n)$ if and only if $\mathcal{N} \vDash \varphi(a_1, \dots, a_n)$.*

Proof. From the substructure, we know they agree on the atomic formulas. So we check the other cases of Δ_0. Negation and conjugation follows. For instance,

$$\mathcal{M} \vDash \neg\varphi \iff \neg(\mathcal{M} \vDash \varphi) \iff \neg(\mathcal{N} \vDash \varphi) \iff \mathcal{N} \vDash \neg\varphi.$$

For bounded quantification, consider $\varphi(y, z_1, \dots, z_n) = \exists x \in y \psi(x, y, z_1, \dots, z_n)$, such that for all $a, a', a_1, \dots, a_n \in M$,

$$\mathcal{M} \vDash \psi(a, a', a_1, \dots, a_n) \quad \Leftrightarrow \quad \mathcal{N} \vDash \psi(a, a', a_1, \dots, a_n).$$

If $M \vDash \varphi(a, a_1, \dots, a_n)$, then there exists $b \in M$ such that

$$\mathcal{M} \vDash \psi(b, a, a_1, \dots, a_n) \wedge b \in a.$$

Then $M \subseteq N$ implies

$$\mathcal{N} \vDash \psi(b, a, a_1, \dots, a_n) \wedge b \in a,$$

and thus $\mathcal{N} \vDash \varphi(a, a_1, \dots, a_n)$.

Now suppose that $\mathcal{N} \vDash \varphi(a, a_1, \dots, a_n)$. Then there exists $b \in N$ such that

$$\mathcal{N} \vDash \psi(b, a, a_1, \dots, a_n) \wedge b \in a.$$

Because $b \in a$ and $a \in M$, by transitivity, we get $b \in M$. So $\mathcal{M} \vDash \psi(b, a, a_1, \dots, a_n) \wedge b \in a$ and by induction we get the result. $\square$

We can extend this theorem a bit. We have just shown that if $\mathcal{M} \subseteq \mathcal{N}$ are transitive and φ is Δ_0, then $\mathcal{M} \vDash \varphi$ if and only if $\mathcal{N} \vDash \varphi$. We also have:

- if φ is Σ_1, then $\mathcal{M} \vDash \varphi$ implies $\mathcal{N} \vDash \varphi$.
- if φ is Π_1, then $\mathcal{N} \vDash \varphi$ implies $\mathcal{M} \vDash \varphi$.

Proposition 21.5. *"x is the empty set" is* Δ_0.

Proof. We can write it as $\forall a \in x \neg(a \in x)$. ☐

Proposition 21.6. *"x is an ordinal" is* Δ_0.

Proof. x is an ordinal if and only if x is transitive and x is well-ordered by $\in$. Transitivity can be written as

$$\forall y \in x \forall z \in y(z \in x)$$

and being well-ordered can be written as a conjunction of things like

$$\begin{gathered} \forall y \in x \exists z \in y(\forall z' \in y(z \in z' \vee z = z')) \\ \exists z \in x \forall z' \in x(z \in z' \vee z = z') \end{gathered}$$

and other stuff. ☐

22 November 17, 2016

Last time, we defined the Lévy hierarchy, where $\Delta_0 = \Sigma_0 = \Pi_0$ are the ones using only bounded quantification.

Proposition 22.1. *Δ_0 formulas are absolute for transitive models. That is, if $\varphi(x_1, \ldots, x_n)$ is Δ_0, $M \subseteq N$ is transitive, and $a_1, \ldots, a_n \in M$, then*

$$M \vDash \varphi(a_1, \ldots, a_n) \leftrightarrow N \vDash \varphi(a_1, \ldots, a_n).$$

We have proved that $\mathrm{empty}(x)$ and $\mathrm{ord}(x)$ are Δ_0, in models of ZF (or even some fragment of ZF). Also $\mathrm{countable}(x)$ is Σ_1, because we can write it as

$$\exists f (f \text{ is an injective function and } \mathrm{im}(f) = \omega \text{ and } \mathrm{dom}(f) = x).$$

We can even see that it is not Δ_0.

Proposition 22.2 (Under Con(ZFC))**.** *$\mathrm{countable}(x)$ is not Δ_0.*

Proof. By downward Löwenhiem–Skolem, there is a countable transitive model $(M, \in) \vDash \mathrm{ZFC}$. Let $\omega_1^{\mathcal{M}} \in M$ be the element such that

$$M \vDash \text{“}\omega_1^{\mathcal{M}} \text{ is the first uncountable cardinal}''.$$

Then $V \vDash \mathrm{countable}(\omega_1^{\mathcal{M}})$ but $M \vDash \neg\mathrm{countable}(\omega_1^{\mathcal{M}})$. □

This is **Skolem's paradox**. That is, if ZFC is consistent, then there are countable models. But ZFC implies that there are uncountable sets. There is also a philosophical argument by Hilary Putnam, about the question "am I a brain in the box?" If I am indeed a brain in the box, then that is from the perspective of the "real" world. But if we ask the question on the "brain in the box" world, the two notions of being a brain in the box doesn't match. So the answer is always no, in a very unsatisfying way.

22.1 Gödel codes

In the beginning of the course, we have said that everything is a set. But we are now talking about formulas. Are these sets? There is a way to code formulas as sets. We can assign to each symbol a different number, to each variable x_n a pair $(1, n)$ and encode like

$$\forall x_n (x_n \in x_m) \quad \text{as} \quad (0, (1, n), 1, (1, n), 2, (1, m), 3).$$

But this is not very satisfactory because this doesn't really match the semantics.

So let us define **Gödel codes** in the following way. Denote by $\ulcorner \varphi \urcorner$ the Gödel code of φ. We first assign numbers to symbols as

$$\begin{array}{llll} \ulcorner (\urcorner = 0, & \ulcorner) \urcorner = 1, & \ulcorner = \urcorner = 2, & \ulcorner \in \urcorner = 3, \\ \ulcorner \neg \urcorner = 4, & \ulcorner \wedge \urcorner = 5, & \ulcorner \exists \urcorner = 6, & \ulcorner x_i \urcorner = (7, i). \end{array}$$

Next we assign codes for formulas inductively as

$$\ulcorner x_i \in x_j \urcorner = (\ulcorner \in \urcorner, \ulcorner x_i \urcorner, \ulcorner x_j \urcorner), \quad \ulcorner x_i = x_j \urcorner = (\ulcorner = \urcorner, \ulcorner x_i \urcorner, \ulcorner x_j \urcorner), \quad \ulcorner \neg\varphi \urcorner = (\ulcorner \neg \urcorner, \ulcorner \varphi \urcorner),$$
$$\ulcorner x_i \wedge x_j \urcorner = (\ulcorner \wedge \urcorner, \ulcorner x_i \urcorner, \ulcorner x_j \urcorner), \qquad \ulcorner \exists x_i \varphi \urcorner = (\ulcorner \exists \urcorner, \ulcorner x_i \urcorner, \ulcorner \varphi \urcorner).$$

Because every code starts with some symbol, we can parse it easily.

Theorem 22.3. *$M \vDash \varphi(a_1, \ldots, a_n)$ is a Σ_1-formula in M, $\ulcorner \varphi \urcorner$, and $a_1, \ldots, a_n$.*

Proof. Later. ☐

22.2 Reflection

Theorem 22.4 (Reflection). *Let $\kappa = \operatorname{cof} \kappa > \omega$ and $\langle (M_\alpha, E_\alpha) : \alpha < \kappa \rangle$ be a sequence of $\{E\}$-structures such that*

(a) $\alpha < \beta$ implies $(M_\alpha, E_\alpha) \subseteq (M_\beta, E_\beta)$,

(b) if α is a limit then $M_\alpha = \bigcup_{\beta<\alpha} M_\beta$ and $E_\alpha = \bigcup_{\beta<\alpha} E_\beta$,

(c) $|M_\alpha| < \kappa$.

Set $M = \bigcup_{\alpha<\kappa} M_\alpha$ and $E = \bigcup_{\alpha<\kappa} E_\alpha$. Then

$$C = \{\alpha < \kappa : (M_\alpha, E_\alpha) \preccurlyeq (M, E)\}$$

*is a **club**[1] in κ.*

Proof. To prove this, we are going to define the **Skolem function** for $M \subseteq N$. For each $\varphi(x, y_1, \ldots, y_n)$, define $f_\varphi : M^n \to M$ such that if $a_1, \ldots, a_n \in M$ then

$$M \vDash \exists x \varphi(x, a_1, \ldots, a_n) \quad \text{implies} \quad M \vDash \varphi(f_\varphi(a_1, \ldots, a_n), a_1, \ldots, a_n)$$

and also $\min\{\beta < \kappa : f_\varphi(a_1, \ldots, a_n) \in M_\beta\}$ is as small as possible. In short, if there exists such a x, we are choosing that x, and if there doesn't exist such a x then we are choosing anything. This requires choice.

In the homework, you proved the following fact:

> If $X = \bigcup_{\alpha<\kappa} X_\alpha$, $|X_\alpha| < \kappa$, and X_α is increasing and continuous, and $\{(f_n : X^{k_n} \to X) : n < \omega, k_n < \omega\}$ is a sequence of functions, then
>
> $$\{\alpha < \kappa : f_n" X_\alpha^{k_n} \subseteq X_\alpha \text{ for all } n < \omega\}$$
>
> is a club.

[1] Recall that C being a club means that, if $X \subseteq C$ is not cofinal then $\sup X \in C$, and C itself is cofinal in κ.

Note that the number of formulas is ω. So we see that

$$C = \{\alpha < \kappa : f_\varphi\text{"}M_\alpha \subseteq M_\alpha \text{ for all } \varphi \in \text{Formulas}(\in)\}$$

is a club.

We now claim that $\alpha \in C$ if and only if $(M_\alpha, E_\alpha) \preccurlyeq (M, E)$. First assume that $(M_\alpha, E_\alpha) \preccurlyeq (M, E)$. If $a_1, \ldots, a_n \in M_\alpha$ and φ is a formula, look at $M \vDash \exists x\varphi(x, a_1, \ldots, a_n)$. If it is false, then $f_\varphi(a_1, \ldots, a_n) \in M_0 \subseteq M_\alpha$ by minimality. If it true, then $M_\alpha \vDash \exists x\varphi(x, a_1, \ldots, a_n)$ and again by minimality, $f_\varphi(a_1, \ldots, a_n) \in M_\alpha$. Therefore $f_\alpha\text{"}M_\alpha \subseteq M_\alpha$.

Now let us show that $(M_\alpha, E_\alpha) \preccurlyeq (M, E)$ assuming that $f_\alpha\text{"}M_\alpha \subseteq M_\alpha$. For atomic formulas, it follows immediately from $(M_\alpha, E_\alpha) \subseteq (M, E)$. Negation and conjunction are more straightforward. For existential quantifiers, this is what the Skolem functions are designed for. If $M_\alpha \vDash \exists x\varphi(x, a_1, \ldots, a_n)$, so does M. If $M \vDash \exists x\varphi(x, a_1, \ldots, a_n)$ then $M \vDash \varphi(f_\varphi(a_1, \ldots, a_n), a_1, \ldots, a_n)$. So $M_\alpha \vDash \varphi(f_\varphi(a_1, \ldots, a_n), a_1, \ldots, a_n)$. $\square$

So this is a set-theoretical version of reflection. There is a more generalized reflection, called the generalized reflection.

Theorem 22.5 (Generalized reflection)**.** *Let $\langle \omega_\alpha : \alpha \in \text{On}\rangle$ be a definable transitive hierarchy. Set $\omega = \bigcup_{\alpha\in\text{On}} \omega_\alpha$. For each formula $\varphi(x_1, \ldots, x_n)$ there is some $\alpha \in \text{On}$ such that for every $a_1, \ldots, a_n$,*

$$(\omega_\alpha, \in) \vDash \varphi(a_1, \ldots, a_n) \leftrightarrow (\omega, \in) \vDash \varphi(a_1, \ldots, a_n).$$

22.3 Constructing the constructible universe

For a transitive structure (M, E) and $X \subseteq M$, define the **definable power set** as

$$\text{Def}^M(X) = \left\{ Y \subseteq X : \begin{array}{c} \exists\varphi(x, y_1, \ldots, y_n) \text{ and } a_1, \ldots, a_n \in M \\ \text{such that } y \in Y \leftrightarrow (M, E) \vDash \varphi(y, a_1, \ldots, a_n) \end{array} \right\}.$$

We now define

$$L_0 = \emptyset, \quad L_{\alpha+1} = \text{Def}^{L_\alpha} L_\alpha, \quad L_\delta = \bigcup_{\alpha<\delta} L_\alpha \text{ for a limit } \delta, \quad L = \bigcup_{\alpha\in\text{On}} L_\alpha.$$

Theorem 22.6 (In ZF)**.**

(1) L is a definable class, i.e, there exists a formula $\varphi(x)$ such that $x \in L \leftrightarrow \varphi(x)$.

(2) $L \vDash (\forall x\varphi(x))$. This "$\forall x\varphi(x)$" is called $\text{V} = \text{L}$.

(3) $L \vDash \text{ZFC} + \text{GCH}$.

Proof of (1). We are going to show that $\exists y(x = \mathrm{Def}^y\, y)$ is a definable formula (and we will even see later that it is Σ_1). Set

$$\begin{aligned}
\mathrm{Lev}(x,y) &= \text{“}\operatorname{ord}(y) \wedge x = Ly\text{”}\\
&= \operatorname{ord}(y) \wedge \exists f \begin{pmatrix} f \text{ is a function with domain } y+1 \wedge \\ f(0) = \emptyset \wedge \\ (\forall \beta \in y+1(\lim(\beta) \to f(\beta) = \bigcup\{f(\gamma) : \gamma \in \beta\}))\wedge \\ (\forall \beta, \beta' \in y+1(\beta = \beta'+1 \to f(\beta) = \mathrm{Def}^{f(\beta')}\, f(\beta')))\wedge \\ f(x) = y \end{pmatrix}.
\end{aligned}$$

This is made so that $f(\alpha) = L_\alpha$ for all $\alpha \in y+1$.

Now $x \in L$ is $\exists \alpha, y(\mathrm{Lev}(y,\alpha) \wedge x \in y)$. This is in Σ_1. $\square$

We are further going to show that L is canonical, in the sense that if $W \subseteq W'$ are models of ZF, then $L^W = L^{W'}$.

23 November 22, 2016

Last time we showed that L is a definable class. We also gave a first order formula "Lev$(x, \alpha) = x \in L_\alpha$". We now want to show that $L \vDash \text{ZF}$ and also $L \vDash \text{V} = \text{L}$.

23.1 L satisfies ZF

Proposition 23.1 ($L \vDash \text{ZF}$). *For each axiom φ of* ZF*,* ZF *proves φ^L (relativisation of φ to L).*

Proof. By one of your homeworks, L is transitive. Then Foundation^L and Extensionality^L holds. Now let us now show that the other axioms are also satisfied. If $x, y \in L_\alpha$, then $\{x, y\} \in L_{\alpha+1}$ because we have

$$\{x, y\} = \{z \in L_\alpha : L_\alpha \vDash (z = x) \vee (z = y)\} \in L_{\alpha+1}.$$

Likewise, we can define the union as

$$\cup a = \{z \in L_\alpha : L_\alpha \vDash \exists y \in a(z \in y)\} \in L_{\alpha+1}.$$

We have $\omega \in L_{\omega+1}$ and so there is an infinite set.

For Power Set, we need to show that for any $a \in L$, $\mathcal{P}(a) \cap L \in L$. This is an interesting statement, because $\mathcal{P}(a) \cap L \neq \text{Def}^{L_\alpha} a$. In fact, we will later show that $\mathcal{P}(\omega) \cap L \subseteq L_{\omega_1}$ but $\mathcal{P}(\omega) \cap L \not\subset L_\alpha$ for $\alpha < \omega_1$. So we have to go up far up into the hierarchy. For $X \subseteq a$, let

$$f(X) = \begin{cases} 0 & \text{if } X \notin L \\ \beta & \text{minimal such that } X \in L_\beta. \end{cases}$$

Then if $\gamma = \sup\{f(X) : X \subseteq a\}$, $\mathcal{P}(a) \cap L \subseteq L_\gamma$. Then

$$\mathcal{P}(a) \cap L = \{z \in L_\gamma : L_\gamma \vDash z \subseteq a\} \in L_{\alpha+1}.$$

The next axiom is Comprehension. If $a, b_1, \ldots, b_n \in L_\alpha$ and $\varphi(x, y_1, \ldots, y_n)$, we want to show that $\{x \in a : L \vDash \varphi(x, b_1, \ldots, b_n)\} \in L$. We have

$$\{x \in a : L_\alpha \vDash \varphi(x, b_1, \ldots, b_n)\} \in L_{\alpha+1},$$

but they are not the same set because of existential quantifiers. So we use the general reflection principle. There exists a $\alpha < \gamma \in \text{On}$ such that for all $b_1', \ldots, b_n', b_{n+1}' \in L_\gamma'$,

$$L_\gamma \vDash \varphi(b_1', \ldots, b_{n+1}') \leftrightarrow L \vDash \varphi(b_1', \ldots, b_{n+1}').$$

Then

$$\{x \in L_\gamma : L_\gamma \vDash x \in a \wedge \varphi(x, b_1, \ldots, b_n)\} \in L_{\gamma+1}.$$

Collection can be proven similarly. $\square$

23.2 Defining definablity

Theorem 23.2. *The formula* $\mathrm{DEF}(x, M) =$ "$x = \mathrm{Def}^M M$" *is a* Σ_1*-formula.*

Corollary 23.3. *(1) If* $W \subseteq V$ *is a transitive, definable model of* ZFC *with* $\mathrm{On} \subset W$*, then* $L = L^W (= \{x : W \vDash \exists\alpha \, \mathrm{Lev}(x, \alpha)\})$.
(2) $L \vDash \mathrm{V} = \mathrm{L}$.
(3) L *is the* $\subseteq$*-minimal model of* ZFC *containing all ordinals.*

Proof. (1) Let $x \in L^W$. Then there exists an $\alpha \in \mathrm{On}^W = \mathrm{On}$ such that $W \vDash$ "$\exists y(x \in y \wedge \mathrm{Lev}(y, \alpha))$". Because Σ_1-formulas are absolutely upward, we have $\exists y(x \in y \wedge \mathrm{Lev}(y, \alpha))$. Then $x \in L_\alpha$. This shows that $L_\alpha^W \subseteq L_\alpha$. Now let us show that $L_\alpha \subseteq L_\alpha^W$ by induction. If $x \in L_{\alpha+1}$, then

$$\begin{aligned} x &= \{z \in L_\alpha : L_\alpha \vDash \varphi(x, a_1, \dots, a_n)\} \\ &= \{z \in L_\alpha^W : L_\alpha^W \vDash \varphi(x, a_1, \dots, a_n)\} \in L_{\alpha+1}^W. \end{aligned}$$

(2) We have $L \subseteq V$. So by (1), $L = L^V = L^L$. Then for any $x \in L^L$,

$$\exists\alpha(L \vDash \exists y(x \in y \wedge \mathrm{Lev}(y, \alpha))).$$

(3) This is clear. □

Let us now prove Theorem 23.2. We are going to try an define the formula $x = \mathrm{Def}^M M$. To prevent the formula from climbing up the hierarchy, we are going to set W to be the "master domain" for quantification. So our strategy is to first quantify everything over W and then at the end set W to be the things we want to actually quantify over.

First suppose $\omega \in W$. Note that $\mathrm{omega}(x) =$ "$x = \omega$" is Δ_0. So we may use ω as a parameter. Define

$$\mathrm{TERM}(x, M, W) = \exists n \in \omega(x = \ulcorner x_n \urcorner) \vee \exists a \in M(x = \ulcorner a \urcorner).$$

Then we define the atomic formulas as

$$\begin{aligned} \mathrm{ATOM}(x, M, W) = \exists y, z \in W(\, &\mathrm{TERM}(y, M, W) \wedge \mathrm{TERM}(z, M, W) \\ &\wedge (x = \ulcorner y = z \urcorner \vee x = \ulcorner y \in z \urcorner)). \end{aligned}$$

Now define a formula sequence

$$\begin{aligned} &\mathrm{FSEQ}(F, \ulcorner\varphi\urcorner, M, W) = \\ &\quad \exists n \in \omega(\text{"}F \text{ is a func. with dom. } n+1\text{"} \\ &\qquad \wedge \forall m \in n+1 \begin{pmatrix} \mathrm{ATOM(F(m), M, W)} \\ \vee\exists k \in m(F(m) = \ulcorner \neg F(k) \urcorner) \\ \vee\exists k, l \in m(F(m) = \ulcorner F(k) \wedge F(l) \urcorner) \\ \vee\exists k \in m \exists i \in \omega(F(m) = \ulcorner \exists x_i F(k) \urcorner) \end{pmatrix} \\ &\qquad \wedge F(n) = \ulcorner\varphi\urcorner). \end{aligned}$$

We now encode the statement of a formula F being built only using variables in $\{x_i : i < n\}$. Let

$$\begin{aligned}
&\mathrm{VLEN}(n, F, M, W) = \\
&\qquad \exists i \in \mathrm{dom}(F)(\,\mathrm{ATOM}(F(i), M, W) \wedge \\
&\qquad\qquad (F(i)(1) = \ulcorner x_{n+1} \urcorner \vee F(i)(w) = \ulcorner x_{n-2} \urcorner)) \\
&\quad \wedge \forall m \in \omega(\exists i \in \mathrm{dom}(F)(\,\mathrm{ATOM}(F(i), M, W) \wedge \\
&\qquad\qquad (F(i)(1) = \ulcorner x_{n+1} \urcorner \vee F(i)(w) = \ulcorner x_{n-2} \urcorner)) \to m \in n).
\end{aligned}$$

Now we define a satisfaction sequence.

$$\begin{aligned}
&\mathrm{SSEQ}(S, F, \ulcorner\varphi\urcorner, M, W) = \\
&\quad \exists n, r \in \omega(\text{“}F, S \text{ are func. with dom. } n+1\text{”} \\
&\qquad \wedge \mathrm{FSEQ}(F, \ulcorner\varphi\urcorner, M, W) \wedge \mathrm{VLEN}(r, F, M, W) \\
&\qquad \wedge \forall m \in n+1(\text{Based on how } F(m) \text{ is formed} \\
&\qquad\qquad \to \text{Form } S(m) \text{ to be all tuples in } M^r \text{ satisfy the formula})).
\end{aligned}$$

Here, satisfying the formula can be written as

$$\mathrm{ATOM}(F(m), M, W) \wedge F(M) = \ulcorner x_i \in x_j \urcorner \to \text{“}S(m) = \{s \in M^r : s(i) \in s(j)\}\text{”}$$

plus

$$\begin{aligned}
&\exists i \in r, k \in m(F(m) = \ulcorner \exists x_i F(k) \urcorner) \\
&\qquad \to S(m) = \{s \in M^r : \exists \bar{s} \in S(k) \forall i' < r(i' = i \to s(i) = \bar{s}(i'))\}
\end{aligned}$$

plus some other things. Then finally we can define satisfaction as

$$\mathrm{SAT}(M, \ulcorner\varphi\urcorner, s, W) = \exists S, F \in W(\mathrm{SSEQ}(S, F, \ulcorner\varphi\urcorner, M, W) \wedge s \in S).$$

Finally, using this, we can define definability as

$$\begin{aligned}
\mathrm{DEF}(x, M) = \exists W(\,&\mathrm{MASTER}(W, M) \\
&\wedge \begin{pmatrix} \forall z \in w \exists \ulcorner\varphi\urcorner \in W, i \in \omega(\mathrm{FVAR}(\ulcorner\varphi\urcorner, \{i\}, M, W) \wedge \forall y \in M \\ (y \in z \leftrightarrow \exists s \in M^r(s(i) = y \wedge \mathrm{SAT}(M, \ulcorner\varphi\urcorner, s, W)))) \end{pmatrix} \\
&\wedge \begin{pmatrix} \forall \ulcorner\varphi\urcorner \in W \exists i \in \omega(\mathrm{FVAR}(\ulcorner\varphi\urcorner, \{i\}, M, W) \to \exists z \in x \forall y \in M \\ (y \in z \leftrightarrow \exists r \in \omega, s \in M^r(\mathrm{SAT}(M, \ulcorner\varphi\urcorner, s, W) \wedge s(i) = z))) \end{pmatrix}).
\end{aligned}$$

We still have to define what the master formula is. We are going to define

$$\begin{aligned}
&\mathrm{MASTER}(W, M) = \exists f \exists x \in W(\\
&\qquad \mathrm{omega}(x) \wedge \text{“}f \text{ is a func. with dom. } \omega\text{”} \\
&\qquad \wedge \forall n \in x(f(n) \subseteq W \wedge f(n) \subseteq f(n+1)) \\
&\qquad \wedge (\text{“everything to start recursive def.”} \subseteq f(0)) \\
&\qquad \wedge \forall n \in x(\text{“if we have elements that could be combined in } f(n) \\
&\qquad\qquad \to \text{ their combination is in } f(n+1)\text{”}).
\end{aligned}$$

This shows that the advertised complexity of the statements are correct.

24 November 29, 2016

So last time we went through a couple of things. The main thing was that $\mathrm{DEF}(x, y)$, which codes $x = \mathrm{Def}^y\, y$ is Σ_1. This gave a formula $\mathrm{Lev}(x, \alpha) \in \Sigma_1$ that codes $x = L_\alpha$. This implies that $L \vDash (\mathrm{V} = \mathrm{L})$ and so is the $\subseteq$-minimal inner model of ZF containing all ordinals. Today we are going to show that $L \vDash$ Choice, and also $L \vDash \forall\lambda(2^\lambda = \lambda^+)$.

24.1 L satisfies Choice

There are many equivalent forms of Choice, and we are going to use the well-ordering one. Note that $x \in L$ if and only if there exist $\alpha \in \mathrm{On}$, a formula $\varphi(y, x_1, \dots, x_n)$ and $a_1, \dots, a_n \in L_\alpha$ such that

$$x = \{y \in L_\alpha : L_\alpha \vDash \varphi(y, a_1, \dots, a_n)\}.$$

To order such elements, we first order formulas. Each $\varphi(x_1, \dots, x_n)$ (with no parameters) is a sequence $\varphi_0, \dots, \varphi_k$ such that each term in the sequence is an atomic formula or the negation or conjunction or existential quantified formula of something before. Now define $<_\tau$ on formulas by:

$$\varphi <_\tau \psi \quad \leftrightarrow \quad \begin{pmatrix} \text{sequence of } \varphi \text{ is shorter than the sequence of } \psi \text{ or} \\ \text{lengths are equal and } \varphi <_{\mathrm{lex}} \psi. \end{pmatrix}$$

Note that two equivalent formulas can be technically different formulas.

Proposition 24.1. *$<_\tau$ well-orders* $\mathrm{Formulas}(\tau)$.

Proof. Given $X \subseteq \mathrm{Formulas}(\tau)$, we can first fine a minimal length and then $<_{\mathrm{lex}}$-minimal of the minimal length formulas, which are going to be finite. $\square$

Now define $<_\alpha$ to be a well-order on L_α by recursion, so that if $\alpha < \beta$, then L_α is an initial segment of L_β. For $\alpha = 0$, we have $L_0 = 0$. So we don't need anything. Suppose $\alpha > 0$. Given $x \in L_\alpha$, set

$$\begin{aligned} \beta_x &= \min\{\beta < \alpha : x \subseteq L_\beta\}, \\ \varphi_x &= \min_{<_\tau}\{\varphi : \exists a_1, \dots, a_n \in L_\beta(x = \{y \in L_\beta : L_\beta \vDash \varphi(y, a_1, \dots, a_n)\})\}, \\ (a_1^x, \dots, a_n^x) &= \min_{<_{\beta_x}}\{(a_1, \dots, a_n) \in L_{\beta_x}^n : x = \{y \in L_\beta : L_\beta \vDash \varphi(y, a_1, \dots, a_n)\}\}. \end{aligned}$$

Now given $x, y \in L_\alpha$, we define the order as

$$x <_\alpha y \quad \leftrightarrow \quad \begin{pmatrix} \beta_x < \beta_y \text{ or} \\ \beta_x = \beta_y \text{ and } \varphi_x <_\tau \varphi_y \text{ or} \\ \beta_x = \beta_y,\ \varphi_x = \varphi_y \text{ and } (a_1^x, \dots, a_n^x) <_{\beta_x}^{\mathrm{lex}} (a_1^y, \dots, a_n^y). \end{pmatrix}$$

Then $<_\alpha$ is a well-ordering of L_α because it is a lexicographic product of well orderings. Also it is clear that the orderings extend each other.

Corollary 24.2. $L \vDash$ Choice.

Proof. Given $x \in L$, find α so that $x \subseteq L_\alpha$. Then $<_\alpha$ restricted to x is a well-ordering. $\square$

I haven't made a big deal out of this yet, but we haven't used Choice in V to show that L satisfies Choice.

Corollary 24.3. Con(ZF) $\to$ Con(ZFC).

Proof. In a model of ZF, build L. Then $L \vDash$ ZFC. $\square$

24.2 Models satisfying $\mathrm{V} = \mathrm{L}$

Before we do that, we have to examine the question of when do transitive models think $M \vDash \mathrm{V} = \mathrm{L}$. Note that $\mathrm{V} = \mathrm{L}$ is just the formula

$$(\mathrm{V} = \mathrm{L}) = \forall x \exists \alpha (\mathrm{ord}(\alpha) \wedge xEy \wedge \mathrm{Lev}(y, \alpha)).$$

The answer is that this holds exactly when $M = L_\delta$ for some δ a limit. In proving this, we are going to use the fact that if $\alpha < \delta$ and δ is a limit, then $L_\delta \vDash \mathrm{DEF}(L_{\alpha+1}, L_\alpha)$. This is one of the homework due Thursday.

Proposition 24.4. *If $M \vDash (\mathrm{V} = \mathrm{L})$ for some transitive M, then $M = L_\delta$ for some limit δ.*

Proof. By definition of $\mathrm{V} = \mathrm{L}$, M contains some ordinals. (Recall that $\mathrm{ord}(\alpha) \in \Delta_0$.) Set $\delta = \mathrm{On} \cap M \neq \emptyset$. Since M is transitive, δ is an ordinal. This is because given $\alpha \in \delta$, we have $\alpha \subseteq \delta$ by transitivity.

We now claim that δ is a limit ordinal. If not, suppose $\delta = \alpha + 1$ so that $\alpha \in M$ is the largest ordinal. Apply $\mathrm{V} = \mathrm{L}$ to α to get $y \in M$ and $\beta \in M$ such that $M \vDash \mathrm{ord}(\beta) \wedge \alpha \in y \wedge \mathrm{Lev}(y, \beta)$. But note that this is a Σ_1 formula. So M is actually right about everything, i.e., $y \in L_\beta$ and $\alpha \in L_\beta$ and so $\beta > \alpha$. This contradicts the maximality of α. So δ is indeed a limit ordinal.

Now we show that $M = L_\delta$. Let $\alpha \in \delta$. There exists $y \in M$ and $\beta \in M$ such that $y = L_\beta$ and $\alpha < \beta$. Then $L_\alpha \subseteq L_\beta \subseteq M$. This shows that $L_\delta = \bigcup_{\alpha<\delta} L_\alpha \subseteq M$. For the other direction, consider an arbitrary $x \in M$. There exist $y, \beta \in M$ such that $x \in L_\beta = y$. Then $\beta \in M \cap \mathrm{On} = \delta$ and so $x \in L_\delta$. Thus $M = L_\delta$. $\square$

We would now like to show that its converse holds. That is, if δ is a limit ordinal then $L_\delta \vDash (\mathrm{V} = \mathrm{L})$.

Lemma 24.5. *If δ is a limit and $\alpha < \delta$, then $\langle L_\beta : \beta < \alpha \rangle \in L_\delta$.*

This allows us to transfer the Σ_1 formula $\mathrm{Lev}(x, \alpha)$ from L to L_δ. Although Σ_1 formulas don't go downwards, this sequence will serve as a witness.

Proof. We use induction on δ. We have three cases: $\delta = \omega$, $\delta = \delta' + \omega$ for some limit δ', and δ a limit of limit ordinals. First look at the case $\delta = \omega$. Then $\alpha < \delta$ is finite, and so L_ω contains all finite sequences of finite things (more precisely, hereditarily finite sets).

It is also easy when δ is the limit of limits. Let $\alpha < \delta$ and then there exists a limit $\delta' < \delta$ so that $\alpha < \delta'$. Then $\langle L_\beta : \beta < \alpha\rangle \in L_{\delta'} \subseteq L_\delta$.

Finally assume that $\delta = \delta' + \omega$. If $\alpha < \delta'$, then we are done. Otherwise, there is some $n < \omega$ such that $\alpha = \delta' + n$. Suppose first that $n = 0$. Then $\alpha = \delta'$. By induction, for every $\beta < \alpha$ we have $\langle L_{\beta'} : \beta' < \beta\rangle \in L_{\delta'}$. This shows that $(\beta', L_{\beta'}) \in L_{\delta'}$, and thus

$$\langle L_\beta : \beta < \alpha\rangle = \{(\beta, L_\beta) : \beta < \alpha\} \subseteq L_{\delta'}.$$

But we want this set as a definable subset. Set $\varphi(x)$ to be

$$\text{“}x = (\alpha', y) \text{ where } \operatorname{ord}(\alpha') \wedge \exists f \begin{pmatrix} \text{function with domain } \alpha' \wedge \\ f(0) = \emptyset \wedge \mathrm{DEF}(f(\beta+1), f(\beta)) \wedge \\ \beta < \alpha \text{ limit} \to f(\beta) = \bigcup_{\beta' < \beta} f(\beta') \end{pmatrix}\text{”}$$

So

$$\langle L_\beta : \beta < \alpha\rangle = \{y \in L_{\delta'} : L_{\delta'} \vDash \varphi(y)\} \in L_{\delta'+1}.$$

Now consider the case $n > 0$, where $\alpha = \delta' + n$. Then $\langle L_\beta : \beta < \delta' + n - 1\rangle \in L_\delta$ by induction. We have $L_{\alpha-1} = \{y \in L_{\alpha-1} : L_{\alpha-1} \vDash (y - y)\} \in L_\alpha$. So we get $(\alpha - 1, L_{\alpha-1}) \in L_{\alpha+5}$ or something. Then adding this element in, we get

$$\langle L_\beta : \beta \in \delta' + n\rangle \in L_\delta.$$

This finishes the proof. $\square$

Theorem 24.6. *If δ is a limit, then $L_\delta \vDash (\mathrm{V} = \mathrm{L})$.*

Proof. Remember this says that $\forall x \exists y, \alpha (x \in y \wedge \operatorname{ord}(\alpha) \wedge \operatorname{Lev}(y, \alpha))$. Let $x \in L_\delta$. There exists some $\alpha < \delta$ such that $x \in L_\alpha$, and by construction, $L_\alpha \in L_\delta$. Now it suffices to show $L_\delta \vDash \operatorname{Lev}(L_\alpha, \alpha)$. Now use the previous lemma with $\alpha + 1$. So $f = \langle L_\beta : \beta < \alpha + 1\rangle \in L_\delta$. We now want to show that

$$L_\delta \vDash \begin{pmatrix} f \text{ is a function with domain } \alpha + 1 \wedge \\ f(0) = \emptyset \wedge \mathrm{DEF}(f(\alpha+1), f(\alpha)) \wedge \\ (\beta \text{ limit } \to f(\beta) = \bigcup_{\beta' < \beta} f(\beta')) \wedge f(\alpha) = L_\alpha \end{pmatrix}.$$

But everything here is Δ_0, because of the things you are going to prove in the homework. Thus L thinking that all these are true implies L_δ thinking that all these are true. $\square$

We are going to prove that this implies $L \vDash \mathrm{GCH}$ next time.

25 December 1, 2016

The plan today is finish talking about L and talk about forcing briefly. Last time we showed that $L \vDash \mathrm{ZFC} + (\mathrm{V} = \mathrm{L})$. Also, we showed that $M \vDash (\mathrm{V} = \mathrm{L})$ if and only if $M = L_\delta$ for some limit δ. The goal is to prove $L \vDash \mathrm{GCH}$.

25.1 L satisfies GCH

Lemma 25.1 (Condensation lemma). *If an infinite set $X \in L$ is transitive, then $X \in L_{|X|^+}$.*

Note that being transitive is very important. There are lots of singletons that show up later in the hierarchy.

Proof. Find a limit δ_0 such that $X \in L_\delta$. We have a structure $(L_\delta, \in)$. Use the Downward Löwenheim–Skolem–Tarksi to find an elementary substructure $(M, E^{\mathcal{M}}) = \mathcal{M} \preccurlyeq (L_\delta, \in)$ such that

- $X \cup \{X\} \subseteq M$,
- $|M| \leq |X|$.

Because $L \vDash (\mathrm{V} = \mathrm{L})$, we have $\mathcal{M} \vDash (\mathrm{V} = \mathrm{L})$. We don't know that M is transitive. But we know that $E^{\mathcal{M}}$ is an extensional well-founded relation. Use Mostowski's theorem to find

$$\pi : (M, E^{\mathcal{M}}) \cong (A, \in)$$

with A transitive. And $A \vDash (\mathrm{V} = \mathrm{L})$. So by last time, $A = L_\gamma$ for $\gamma = \mathrm{On} \cap A$ a limit ordinal. Then $|\gamma| \leq |A| = |M| = |X|$. So $\gamma < |X|^+$ and $A \subseteq L_{|X|^+}$.

But we are not there yet, because we want $X \in L_{|X|^+}$. We claim that $X \in A$. Recall that $X \in M$ is transitive and for all $x \in M$, $\pi(x) = \{\pi(y) : y \in M, \mathcal{M} \vDash yEx\}$. By induction on rank, for all $x \in X \cup \{X\}$, $\pi(x) = x$. This is because $\pi(\emptyset) = \emptyset$ and $\pi(x) = \{\pi(y) : y \in x\} = \{y : y \in x\} = x$. This shows that $\pi(X) = X \in A$. $\square$

Theorem 25.2. $L \vDash \mathrm{GCH}$.

Proof. Let us work in L. Let λ be a cardinal (i.e., let $\lambda \in L$ such that $L \vDash$ "λ is a cardinal"). We claim that $\mathcal{P}(\lambda) \subseteq L_{\lambda^+}$. Let $X \in \mathcal{P}(\lambda)$. Then $\{X\} \cup \lambda$ is checked to be transitive. By condensation, we have $\{X\} \cup \lambda \in L_{\lambda)}$ and so $X \in L_{\lambda^+}$. Then $|\mathcal{P}(\lambda)| \leq |L_{\lambda^+}| = \lambda^+$. $\square$

Corollary 25.3. $\mathrm{Con}(\mathrm{ZF}) \to \mathrm{Con}(\mathrm{ZFC} + \mathrm{GCH} + \mathrm{V} = \mathrm{L})$.

25.2 Forcing

So far, we have done everything by constructing L. But we don't know how to do the other direction. This is done by forcing.

Theorem 25.4. $\mathrm{Con(ZF)} \to \mathrm{Con(ZFC} + \neg\,\mathrm{GCH} + \mathrm{V} \neq \mathrm{L})$.

Because I have an hour, I can going to try to give at least a flavor of forcing. It will lack details and ignore metamathematical issues.

Assume we have a countable, transitive model M of ZFC. We want to build a transitive $N \supseteq M$ such that

- $N \vDash \mathrm{ZFC}$,
- $\mathrm{On} \cap M = \mathrm{On} \cap N$,
- N is built in a "controlled fashion".

Here is the outline. Start with a partial order $\mathbb{P} \in M$ and find a M-generic filter $G \notin M$. Then form $M[G] \supseteq M \cup \{G\}$, and argue in general $M[G] \vDash \mathrm{ZFC}$. Finally use the properties $\mathbb{P}$ to conclude something.

Let $\mathbb{P} \in M$ be a partial order, and assume that $\mathbb{P}$ has a greatest element $1_{\mathbb{P}} \in \mathbb{P}$. (This is a Δ_0 statement.) We say that a subset $D \subseteq \mathbb{P}$ is **dense** if and only if for every $p \in \mathbb{P}$, there is a $q \in D$ such that $q \leq p$. We also say that $G \subseteq \mathbb{P}$ is a **filter** if

- $\forall p \in \mathbb{P}, q \in G(q \leq p \to p \in G)$,
- $\forall p, q \in G(\exists r \in G(r \leq p, q))$.

A filter G is called M**-generic** if for all dense $D \in M$, $G \cap D \neq \emptyset$.

Proposition 25.5. *If M is a countable transitive model and $\mathbb{P} \in M$, then there exists a M-generic filter $G \notin M$.*

Assume, given a M-generic G, we can build a countable transitive $M[G] \supsetneq M \cup \{G\}$ such that $M[G] \vDash \mathrm{ZFC}$ and $M \cap \mathrm{On} = M[G] \cap \mathrm{On}$. We assume this as a black box for now.

Take $\mathbb{P} = \mathrm{Add}(\omega, 1) \in M$. Then $D_{n,\alpha}, \mathrm{Diff}_{\alpha,\beta}, D^A_\alpha \in M$ for $n < \omega, \alpha = 0$, and $A \in \mathbb{P}(\omega) \cap M$. If G is M-generic, it meets all of these. Then $\bigcup G : 1 \times \omega \to 2$ is a function. Define

$$X = X_0^G = \{n < \omega : \bigcup G(0, n) = 1\} \subseteq \omega.$$

But $X \neq A$ for $A \in M$. So $M[G]$ contains a subset of ω that M doesn't.

Theorem 25.6. $M[G] \vDash (\mathrm{V} \neq \mathrm{L})$.

Proof. $L^{M[G]} = L^M \subseteq M$. But $X \in M[G] - L^{M[G]}$. □

Here we added only one element. But we can do more than this. Find an $\alpha \in M$ such that $M \vDash$ "$\alpha > \omega_1$ is a cardinal". Set $\mathbb{P} = \mathrm{Add}(\omega, \alpha)^M \in M$. Find a M-generic $G \subseteq \mathbb{P}$ and form $M[G]$. From G, we get

$$M[G] \vDash \text{"}\exists \text{ injection from } \alpha \text{ to } \mathcal{P}(\omega)\text{"}.$$

So $M[G] \vDash$ "$2^\omega \geq \alpha$". We would like to show that $M[G] \vDash$ "$\alpha > \omega_1$". But this statement is Σ_2 or something, and so we can't say this directly. But it turns out that $M[G]$ still thinks this is true. This is because $\mathrm{Add}(\omega, \alpha)^M$ has the countable chain condition. If $\mathbb{P} \in M$ has the countable chain condition and $G \supseteq \mathbb{P}$ is M-generic, then M and $M[G]$ have the same cardinalities and the same cofinalities. This means that $M[G] \vDash$ "$\alpha > \omega_1$ is a cardinal". These two combined shows that $M[G] \vDash \neg\,\mathrm{CH}$.

You can run the same argument by using κ instead of ω although it becomes more complicated. Also use can do it more than one cardinal at a time.

Theorem 25.7 (Easton)**.** *Suppose M satisfies F is a (definable class) such that for all $\kappa, \lambda \in \mathrm{dom}\, F$,*

(1) $\kappa < \lambda \to F(k) \leq F(l)$*,*

(2) $\mathrm{cof}(F(\kappa)) > \kappa$*,*

(3) κ *regular.*

Then there exists a $\mathbb{P} \in M$ such that for all M-generic $G \subseteq \mathbb{P}$,

$$M[G] \vDash \text{"}\forall \kappa \in \mathrm{dom}\, F(2^\kappa = F(\kappa))\text{"}$$

and M and $M[G]$ have the same cardinals and cofinalities.

We are going at least open the black box and look inside. So what is $M[G]$? Fix a $\mathbb{P} \in M$. Define a $\mathbb{P}$-name as, $\dot{x}$ is a $\mathbb{P}$**-name** if and only if

$$\dot{x} = \{(\dot{y}, p) : p \in \mathbb{P}, \dot{y} \text{ is a } \mathbb{P}\text{-name}\}.$$

Given a $\mathbb{P}$-name $\dot{x}$ and a M-generic filter G, we define

$$\dot{x}^G = \{\dot{y}^G : (\dot{y}, p) \in \dot{x}, p \in G\}$$

and $M[G] = \{\dot{x}^G : \dot{x} \in M \text{ is a } \mathbb{P}\text{-name}\}$.

For each $x \in M$, we can define a canonical name $\check{x}$ by

$$\check{x} = \{(\check{y}, 1_{\mathbb{P}}) : y \in x\}.$$

Then $\check{x}^G = x$ and so $M \subseteq M[G]$. Also $\dot{\Gamma} = \{(\check{p}, p) : p \in \mathbb{P}\}$. Then for all $G \subseteq \mathbb{P}$, $\dot{\Gamma}^G = G \in M[G]$.

Forcing black box. *Let $\mathbb{P} \in M$ be a p.p. Then there is a definable relation $\Vdash$ such that $\forall \dot{a}_1, \ldots, \dot{a}_n \in$ Name and $p \in \mathbb{P}$ and $\varphi(x_1, \ldots, x_n)$, the following are equivalent:*

(1) $M \vDash$ "$p \Vdash \varphi(\dot{a}_1, \ldots, \dot{a}_n)$"*.*

(2) For any M-generic G with $p \in G$, $M[G] \vDash \varphi(\dot{a}_1^G, \ldots, \dot{a}_n^G)$.

The book has more detailed exposition to forcing.

Index