Math 145a Lecture Notes

Evan Chen
evanchen@college.harvard.edu

Harvard College
Fall 2014

This is Harvard College's *Math 145a*, instructed by Peter Koellner. The formal name for this class is "Set Theory I".

The permanent URL is http://web.evanchen.cc/coursework.html, along with all my other course notes.

Contents

§1 September 2, 2014

§1.1 Broad Overview

The text for this course is *Set Theory*, by Koellner, which I just downloaded. The **grading** for this course is 100% problem sets.

The course has three parts,

- an introduction to set theory,
- the constructible universe,
- the Solovay model and forcing.

The goal of the course is the second and third part, in which we prove some things are independent. For example, CH is independent of ZFC.[1]

Today we'll be talking about the notion of independence.

§1.2 Introduction to Independence

This is "chapter 0", not yet in the text.

There are, very broadly, two kinds of mathematics.

1. Algebraic, which is not in general concerned with a specific structure. For example, group theory or theory of rings, topology, and so on. These topics are not about *specific* structures like $\mathbb{N}$.

2. In contrast, non-algebraic stuff is concerned with a specific structure. For example, number theory cares a lot about $\mathbb{N}$. (In a bit, we will show that $(\mathbb{N}, 0, S, +\times)$, where S is a successor function, is unique up to isomorphism.) As another example, analysis, which cares about $(\mathcal{P}\mathbb{N}, \in)$. Note that $2^{\mathbb{N}} \sim \mathbb{R}$. As a third example, functional analysis cares about $(\mathcal{P}\mathcal{P}\mathbb{N}, \in)$.

Set theory is the second type, and we care about iterating $\mathcal{P}$. Iterating n times gives V_n.

- V_n is finite combinatorics.
- $V_\omega \sim \mathbb{N}$
- $V_{\omega+1} \sim \mathcal{P}\mathbb{N}$.

§1.3 Example of Independence

Take the axioms of group theory: given $(G, \cdot)$ we require

(1) $\forall x, y$, $xy \in G$

(2) $\forall x, y, z$ we have $x(yz) = (xy)z$

(3) $\exists 1 \in G$: $\forall x, x \cdot 1 = 1 = 1 \cdot x$

(4) $\forall x \in G$, $\exists y \in G$ with $xy = 1 = yx$.

Consider (5), G is abelian (meaning $xy = yx$)

[1] Axioms of infinity makes certain things more answerable. ZFC "can't articulate large enough objects". We can introduce larger and larger infinities, much like a "name the larger number" game that small children play.

Fact. The "abelian" statement is independent of the group axioms (1) through (4).

Proof. There exist both abelian ($\mathbb{Z}$) and non-abelian (D_6) groups. Duh. □

So this is not a big deal in algebra, because there are tons of groups, and no one was trying to determine whether "THE group" was abelian.

On the other hand, independence in Euclidean geometry might be a bit more surprising – we now know the parallel postulate is independent of the other four of Euclid's axioms.[2] That's because we're talking about ONE THING. Of course now we have like non-Euclidean geometry, and geometry as a formal discipline became just like group theory.

So once we discovered the parallel postulate was independent of the other four, geometry fractured into "formal" geometry and "applied" geometry.

Philosophical question now: do we have independence with "fixed" structures?

§1.4 More Surprising Examples

Let's take number theory! This has a fixed structure, $(\mathbb{N}, 0, S)$.

The axioms of this structure are denoted PA, the Peano axioms. This again has five axioms.

(1) 0 is a number.

(2) If x is a number, so is $S(x)$.

(3) $S(x) \neq 0$ for any x.

(4) $S(x) = S(y) \implies x = y$.

(5) (Least Criminal) If 0 has property φ (denoted $\varphi(0)$), and $\forall x : \varphi(x) \implies \varphi(Sx)$, then $\varphi(x)$ holds for all x.

The last axiom is the one that's doing all the work – ∞ is packaged in the first four axioms.

Again, the principle is that the resulting structure is FIXED. In the "second order" form of the axioms, PA determines $\mathbb{N}$ up to isomorphism. So there "should" not be undecidable things!

Question 1.1. Is PA complete?[3] In other words, is it the case that for any sentence φ (in the language of PA) that either $\text{PA} \vdash \varphi$ or $\text{PA} \vdash \neg\varphi$?

Here $\text{PA} \vdash \varphi$ means PA proves φ.

So the answer is Gödel's incompleteness theorems – no.

Theorem 1.2 (Gödel's First Incompleteness Theorem)
Assume that PA is consistent. Then there exists a φ such that PA can neither prove φ nor $\neg\varphi$.

Remark. Gödel had to assume a tiny bit more. The above statement is Rösser's version.

[2] Note that Euclid's axioms suck. There are twenty-one Tarski axioms.
[3] Tarski's geometry is complete – there is only "one" Euclidean geometry.

Theorem 1.3 (Gödel's Second Incompleteness Theorem)
Assume PA is consistent. Then PA cannot prove its own consistency.

One can express "PA is consistent" in the language of Peano arithmetic. This is a lot like the "liar" paradox: namely "this sentence is false". Similarly, we construct a statement "I'm not provable".

This is like bad. Outside of PA we can see the truth of PA, but not from within itself.

§1.5 Escaping

It's not enough to add Con(PA) to the system. Gödel's Theorem generalizes as follows.

Theorem 1.4
For any extension T of PA, T cannot prove $\operatorname{Con}(T)$.

§1.6 Models and Compactness

Theorem 1.5 (Gödel, Compactness)
Suppose T is a formal system such that every finite fragment of T has a model. Then T has a model (i.e. it is consistent).

Consider the following: let us add a constant symbol $\dot{c}$ to the language of PA. Let T be the following list of axioms:

- PA
- $\dot{c} \neq 0$
- $\dot{c} \neq 1$
- $\dot{c} \neq 2$
- $\dots$

Obviously every finite fragment of T has a model. So T has a model! Let's call this model

$$(M, 0, S, \dot{c}).$$

The axioms of Peano arithmetic implies we have $S(\dot{c})$, $S(S(\dot{c}))$. That means there are "strange" numbers in addition to this chain of fake numbers hanging out on the side.

§1.7 Looking Ahead

For set theory,we have a system, ZFC. By Gödel, we know if ZFC is consistent, then ZFC cannot prove its own consistency.

However, we can find worse examples.

Question 1.6 (Continuum Hypothesis)**.** Is there an infinite subset $A \subset \mathbb{R}$ such that $A \not\sim \mathbb{N}$ and $A \not\sim \mathbb{R}$?

Theorem 1.7 (Gödel, 1938)
If ZFC is consistent, then ZFC cannot refute CH.

Theorem 1.8 (Cohen, 1965)
If ZFC is consistent, then ZFC cannot prove CH.

This is really terrible because CH does not refer to the system of axioms at all (unlike Con(PA) or Con(ZFC)).

We also have the following fact.

Fact 1.9. Up to isomorphism, $(\mathbb{R}, <)$ is the unique dense linear ordering without endpoints that is separable (i.e. has a countable dense subset).

Hint: it's $\mathbb{Q}$.

Remark. Separable implies every disjoint sequence of intervals is countable.

Question 1.10 (Suslin's Hypothesis)**.** Is the above theorem still true if we replace "separable" with the weaker condition that "every disjoint sequence of intervals is countable"?

This is again independent of ZFC.

These two questions are pretty unfortunate because this time, we have picked the question "before" the choice of axioms (namely ZFC).

§1.8 So what happens in this class?

1. Part 1 of the course will talk about ZFC.
2. Part 2 of the course ("the constructible universe") will deal with Gödel's proof that ZFC cannot refute CH.
3. Part 3 of the course ("forcing") will deal with Cohen's proof that ZFC cannot prove CH.

§2 September 4, 2014

This class is pretty flexible. Anyways, here is an informal introduction to the notions of set theory.

§2.1 Sets

First we contrast *sets* and *concepts*. Examples of concepts are:

- "is red" – applies to red things
- "is a human being"
- "is a featherless biped"

These concepts apply to various things. By the way, the two latter things apply to the same thing, Homo Sapiens. However, they are *different concepts*.

Sets do NOT have this feature.

$$\{\text{Adam}, \text{Eve}, \dots\} = \{\text{featherless bipeds}\}.$$

Hence given the set, we cannot tell what concept created it. In other words:

> *Sets are determined by their elements, while concepts are not determined by the things falling under them.*

Remark 2.1. Sets are *extensional*, which means

$$A = B \text{ iff } \forall x \, (x \in A \iff x \in B).$$

This is the formalization of the above notion.

§2.2 Subsets

Consider $\mathbb{N} = \{0, 1, 2, 3, \dots, \}$. We can consider subsets – write

$$A \subset B \text{ iff } \forall x \, (x \in A \implies x \in B).$$

Let $E = \{0, 2, 4, \dots\} \subset \mathbb{N}$ and $O = \{1, 3, 5, \dots\} \subset \mathbb{N}$. Note that $E \cap O = \varnothing = \{\}$.

The key operation is considering all subsets. Consider all subsets $\mathbb{N}$, including E and O. Notice that E and O are *definable*. Unfortunately there are only countably many definable sets (while $2^{\mathbb{N}} \sim \mathbb{R}$ is uncountable). However, we are still interested in the undefinable sets.

Put

$$\mathcal{P}(\mathbb{N}) = \{A : A \subseteq \mathbb{N}\}$$

as the power set of $\mathbb{N}$. (Here $\mathcal{P}(X)$ is defined analogously.)

§2.3 Cantor's Theorem

Some useful notions (er, more like review):

- Given $f : A \to B$, we say f is *onto* or *surjective* if $f(A) = B$.
- Moreover, f is *one-to-one injective* if it never collapses elements; $\forall x, y \in A \, (x \neq y \implies fx \neq fy)$.
- Finally, f is *bijective* if f is both one-to-one and onto.

Definition 2.2. Two sets A and B have the same size if and only if $\exists f : A \to B$ which is one-to-one and onto.

This lifts this criterion up to infinite sets. If you leave a knife and fork for each person at a table (possibly infinitely large) then there are the same number of knives and forks.

Example 2.3

As above, $E \sim \mathbb{N} \sim O$. Also, $\mathbb{Q} \sim \mathbb{N}$.

Theorem 2.4 (Cantor)

$\mathbb{N} \not\sim \mathbb{R}$.

Proof. Hmm this is a new one. Assume for contradiction we can enumerate the reals as $x_1, \dots$.

Consider the following sequence of nested closed intervals. Start with $I_0 = [0, 1]$. Let $I_1 = [a_1, b_1]$ be such that $b_1 - a_1 \le \frac{1}{1}$ and $x_1 \notin [a_1, b_1]$. Then set $I_2 = [a_2, b_2] \subseteq I_1$ with $b_2 - a_2 \le \frac{1}{2}$ and $x_2 \notin I_2$. Continue.

This gives rise to a nested sequence of intervals

$$I_0 \supset I_1 \supset \dots.$$

By design, $x_n \notin I_n$ for any n. However these intervals are all closed, so $\bigcap_{n \ge 0} I_n = \{x\}$ for some x. Hence this x is not of the form x_k, contradiction. □

This generalizes as follows.

Theorem 2.5

For any set X, $\mathcal{P}(X) \not\sim X$.

Proof. Barber paradox. Also on our Math 55 pset. □

Now that the review is done, let's state some philosophy.

> *The idea of $\mathcal{P}(X)$ is one of the two key ideas of set theory.*

Now what's the second idea?

§2.4 Informal comprehension principle

The **informal comprehension principle** states the following: if X is a set and P as a definite[4] property of elements in X, then there exists a set Y which contains all and only the elements P holds for. In other words,

$$Y = \{x \in X : P(x)\}$$

is a set. Another name is the "informal separation principle".

[4] An example of non-definite property is "is bald". The hallmark of a vague property is that it doesn't obey induction. If a person with n hairs is bald, is someone with $n+1$ hairs bold?

Example 2.6

Take $X = \mathbb{N}$. Then D is even.

Remark 2.7. Note that this does NOT imply that all sets are generated by comprehension. Indeed, if there are only countably many properties, so some subsets of $\mathbb{N}$ are necessarily not generated by properties.

§2.5 Empty set

Definition 2.8. Define $\varnothing = \{x : x \neq x\}$.

The empty set has the very important property that *it is a subset of everything.*
We could have started with $\mathbb{N}$. Specifically,

- $\mathbb{N}$ is where all number theory happens.
- $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$ is where all algebra happens.
- $\mathcal{P}(\mathcal{P}(\mathbb{N})) \sim \{f : \mathbb{R} \to \mathbb{R}\}$ is where all algebra happens.

But we start lower. We have

$$\begin{aligned} V_1 &= \mathcal{P}(\varnothing) = \{\varnothing\} = \{\{\}\} \\ V_2 &= \mathcal{P}(\mathcal{P}(\varnothing)) = \{\varnothing, \{\varnothing\}\} \\ V_3 &= \mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing))) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}. \end{aligned}$$

Notice that in general, the nth iteration is a power tower of 2's:

$$\left|\mathcal{P}^5(\varnothing)\right| = 2^{2^{2^2}} = 2^{16} = 65536.$$

These numbers get quite big quite quickly.
Let's give these things a name.

Definition 2.9. Let $V_0 = \varnothing$ and $V_{n+1} = \mathcal{P}(V_n)$.

Despite how large these numbers are, the collection of $\{V_n\}_n$ is pretty countable. Define

$$V_\omega = \bigcup_{n<\omega} V_n.$$

Then $\mathbb{N} \sim V_\omega$, $\mathbb{R} \sim V_{\omega+1}$, and we recover our ladder.
Note that Cantor's Continuum Hypothesis is that there are no cardinalities between $|V_\omega|$ and $|V_{\omega+1}|$.

§2.6 Well-Orderings

Definition 2.10. Suppose $\prec$ is a binary relation (whatever that means) on a set X. Then $\prec$ is **well-founded** if and only if every non-empty subset Y of X has an $\prec$-minimal element. Moreover, $\prec$ is **well-ordered** if it is well-founded, strict, linear.

Example 2.11

The relation "is an ancestor of" on humans is well-founded. Similarly, $<$ is well-founded on $\mathbb{N}$. However, $>$ is not well-founded over $\mathbb{N}$.

§2.7 Ordinals

Are there larger examples?

Let ω be the next ordinal after all the nonnegative integers. If we want to be formal, $\omega = \{0, 1, 2, 3, \dots\}$. We can then posit $\omega + 1$, and keep going. Thus we have

$$0 < 1 < 2 < \dots < \omega < \omega + 1 < \dots$$

Another similar vein is re-ordering the integers as

$$0 < 2 < 4 < 6 < \dots < 1 < 3 < 5 < \dots$$

which is certainly a valid ordering. These have the same *order type* – there is an obvious order-preserving bijection between them. Thus we focus on the former, which are called the ordinals.

Exercise. Check that these are well ordered! It's an finite way down, but possibly an infinite way up.

Let's start talking about ordinals (keeping in mind everything up to now is still informal).

$$\begin{aligned}
&0,1, 2, 3, \dots, \omega \\
&\quad \omega + 1, \omega + 2, \dots, \omega + \omega \\
&\quad 2\omega + 1, 2\omega + 2, \dots, 3\omega \\
&\quad \vdots \\
&\quad \omega^2 + 1, \omega^2 + 2, \dots \\
&\quad \vdots \\
&\quad \omega^3, \dots, \omega^4, \dots, \omega^\omega \\
&\quad \vdots,
\end{aligned}$$

Here I'm abusing notation. The notion 2ω should be $\omega + \omega$; the notion ω^2 should be $\omega \cdot \omega$, but you get the idea.

We finish with $\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}$ here ω many times, which is called ε_0. In general, ε_{k+1} is ε_k stacked k times. Then we get to $\varepsilon_{\varepsilon_0}$, and so on...

Remark 2.12. Compute $\omega^{\varepsilon_0} = \varepsilon_0$. Actually, ε_0 is the least α such that $\omega^\alpha = \alpha$.

Transfinite induction with ε_0

§2.8 The Hierarchy

Let V be the universe of sets. Iterate $\mathcal{P}$ along *all* the well-orderings.

Later we'll see the following:

- $V_0 = \varnothing$
- $V_{\alpha+1} = \mathcal{P}(V_\alpha)$ (successor)
- $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ if λ is a limit
- $V = \bigcup_{\alpha \in \mathrm{On}} V_\alpha$.

Here On is the order types of everything. We'll show soon $\mathrm{On} \not\subset \mathrm{On}$ and $V \notin V$.

Evan Chen
evanchen@college.harvard.edu (Harvard College Fall 2014)

§3 September 9, 2014

§3.1 Housekeeping

- Office hours: Tuesday 2PM - 3PM, 414 2 Arrow Street
- Book: *A Course in Set Theory*, by Ernest S
- Email professor: background (logic, ST, math) and what you would like to see

Exercises coming next week.

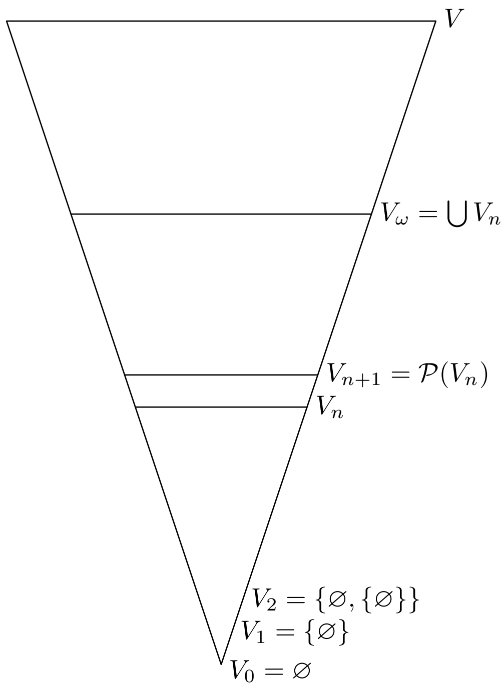
§3.2 Last Time

Subject matter: set theory hierarchy.

Three fundamental ideas:

- Well-ordering (ordinals)
- Power set
- Absolute infinity, which we'll discuss more below.

The hierarchy V is built up in stages from $\varnothing$, by taking the power set of the previous stage. This picture has shown up so many times I will actually draw it.



ε_0: this is what forever really is. :D Except ε_0 is supposedly "piddling". darn.

§3.3 Quasi-philosophical interlude

Some people (potentialists) think that

- The power set of an infinite set (like $\mathbb{N}$) is "open-ended". We call these width potentialists.

- The height of the universe (ordinals) is "open-ended". We call these height potentialists.

Why would someone think $2^{\mathbb{N}}$ is open-ended? We showed that $|\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$ already. Some people think the idea $\mathcal{P}(\mathbb{N})$ does not even make sense. The potentialists think that subsets of $\mathbb{N}$ which are definable make sense but are skeptical of the notion of "all" subsets of $\mathbb{N}$.

Consider a binary branching tree which represents decisions on whether to include an element of $\mathbb{N}$. (Going right at the nth step means including n in.)

Anyways the opposite of a potentialist is an actualist.

§3.4 Categoricity

We now show the philosophy is a moot point. Suppose we have two hierarchies $V_0, V_1, \dots$ and $V_0', V_1', \dots$. Since $\mathbb{N}$ is isomorphic in these things, there as an isomorphism of V_ω to V_ω'. Now in my sense

$$V_{\omega+1} = P^V\left(V_\omega\right).$$

In your sense

$$V_{\omega+1}' = P^{V'}\left(V_\omega'\right).$$

But any A specified in V_ω leads to a set of V_ω'.

OK I have no idea what this is. But it was informal. The point is going to be categoricity. Regardless of what makes sense and what does not, apparently everything is isomorphic?

§3.5 Language of Set Theory

OK whatever, let's consider the universe V.

In number theory, we defined the integers through a successor function. The analog here is the power set operator $\mathcal{P}$.

We now enter the domain of Chapter 1, the language of set theory. Firstly it ni the language of logic. This includes $\forall$, $\exists$, an infinite supply of variables, as well as negation $\neg$, $\wedge$, $\vee$, and finally $\to$ and $\leftrightarrow$. Moreover, we have a symbol $=$.

You can't say too much with this; in Number Theory we solve this problem by defining a few extra things, 0 and the successor function S, among other things. In set theory we add only one symbol: the membership $\in$. For example, consider

$$\forall x \exists y (x \in y).$$

This has important implications: we can already generate $\mathbb{N}$ by

$$x \in y_0 \in y_1 \in y_2 \in \dots$$

Now we can prepare the axioms.

§3.6 The First Five Axioms

First, we distinguish a set from a concept.

Axiom I (Extensionality)**.** A set is determined by its elements, meaning

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

Now we need to begin somewhere.

Axiom II (Empty Set)**.** The empty set exists: $\exists x \forall y (y \notin x)$.

By Extensionality, there is only one such empty set, and we denote it by $\varnothing$.

Axiom III (Pairing)**.** Informally, for any x, y we can create $\{x, y\}$. Formally,

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

Again by Extensionality, this set is unique, and we denote it by $\{x, y\}$.

Axiom IV (Union)**.** Informally, we can take $\bigcup_{a' \in a}$. Formally,

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

Again by Extensionality (see a pattern here?), this is unique, so we call it $\bigcup x$.

Example 3.1

If $x = \{\mathbb{N}\}$, $\bigcup x = \mathbb{N}$. So that means using union, we can generate large sets from small ones.

Now for the power set.

Axiom V (Power Set)**.** We can construct $\mathcal{P}(x)$. Formally,

$$\forall x \exists a \forall y (y \in a \leftrightarrow y \subseteq x)$$

where $y \subseteq x$ is short for $\forall z (z \in y \rightarrow z \in x)$.

Again, we do not have a lot of symbols, so we define lots of shorthands like $\subseteq$. The important thing is that this in principle can be expanded. Anyways, we denote this by $\mathcal{P}(x)$ since it is unique by Extensionality.

§3.7 The Sixth Axiom, Infinity

Note that the first five axioms are already sufficient to construct

$$\mathcal{P}(\mathcal{P}(\dots(\varnothing))).$$

This lets us get up to the natural numbers.

Moreover, remark that $V_\omega = \bigcup_{n \in \mathbb{N}} V_n$ is a model for these axioms. Just check all the axioms hold.

But V_ω is countable, and all the sets are freaking finite. Boring! Let's force infinitely large sets.

Axiom VI (Infinity)**.**

$$\exists x \left(\varnothing \in x \wedge \forall y \left(y \in x \rightarrow y \cup \{y\} \in x\right)\right).$$

This time we can't conclude x is unique. But we can deduce some things:

$$\begin{aligned} \varnothing \in x &\implies \{\varnothing\} \in x \\ &\implies \{\varnothing, \{\varnothing\}\} \in x \\ &\implies \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \in x \\ &\dots \end{aligned}$$

Actually, each line is just the union of the objects on all the previous lines. This is a lot like ω, where we define $\omega = \{0, 1, 2, \dots, \}$ and $\omega + 1 = \{0, 1, 2, \dots, \omega\}$. Basically, the way we generate a new object is to take the set of all previous objects.

Anyways, x is not unique. We can throw in $\{\{\varnothing\}\}$ in or something, and suddenly we get more junk in x. However, there is nonetheless a minimal x. Here's how we get our hands on it: Call a set x *inductive* if

$$\varnothing \in x \wedge \forall y \, (y \in x \to y \cup \{y\} \in x) \, .$$

Then define $\omega = \bigcap \{A \mid A \text{ inductive}\}$. (We'll define $\bigcap$ later).

§3.8 The Seventh Axiom, Foundation

Now we will make induction work by ruling out infinite chains.

Axiom VII (Foundation)**.**

$$\forall x \, (x \neq \varnothing \to \exists y \in x \forall z \in x (z \notin y)) \, .$$

Equivalently, "there are no infinite descending $\in$ chains".

This is not too hard to see. Suppose

$$x_1 \ni x_2 \ni x_3 \ni \dots$$

Then take $x = \{x_k\}_{k \ge 1}$, which fails Foundation. Conversely, if Foundation fails then it is not hard to generate an infinite $\ni$ chain.

Anyways, what is a model for this? If we take the universe $V_{\omega+1} = \mathcal{P} V_\omega$, it turns out that this satisfies Infinity, because $V_\omega \in V_{\omega+1}$. However, it doesn't satisfy Power Set anymore, because $\mathcal{P}(V_{\omega+1})$ is not in there. Nonetheless, we can extend this up to $V_{\omega+\omega}$, and now we have a model!

You might ask why we don't just stop at $V_{\omega+\omega}$. Mainly, because we can. Like, FLT was not proved in ZFC. If you give yourself more machinery, you can prove more stuff.

§3.9 The Last Infinitely Many Axioms, Replacement

ZFC does not have eight axioms, it has infinitely many! We just like to condense this as replacement.

Axiom VIII (Replacement)**.** For each formula φ in the Language of Set Theory, and for every positive integer n,

$$\begin{aligned} &\forall p_1 \forall p_2 \dots \forall p_n \forall a \, [\forall y \in a \; \exists! z \; \varphi(y, z, p_1, p_2, \dots, p_n)] \\ &\qquad \to [\exists b \, \forall z \, (z \in b \leftrightarrow \exists y \in a \; \varphi \, (y, z, p_1, \dots, p_n))] \, . \end{aligned}$$

What is this saying? Really φ defines a function F (relative to the parameters p_i) on domain a, then we can collect them together in a set $b = F(a)$.

It turns out the Replacement does not hold in $V_{\omega+\omega}$ because there is no set

$$\{V_\omega, V_{\omega+1}, V_{\omega+2} \dots\} \, .$$

Actually, Replacement blows the top off this, making ε_0 seem small. Oops.

§4 September 11, 2014

Happy 18th birthday, Jessica!

In what follows, we will just abbreviate $\varphi(x, p_1, \dots, p_n)$ as $\varphi(x)$.

§4.1 Defining the nonnegative integers

Last time we introduced ZF and the language of set theory.

First, let us actually define

$$\begin{aligned} 0 &= \varnothing \\ 1 &= \{\varnothing\} \\ 2 &= \{\varnothing, \{\varnothing\}\} \\ 3 &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \end{aligned}$$

and in general, $n+1 = \{0, 1, \dots, n\}$. Then $\omega = \bigcup_{n \in \mathbb{N}} n$.

§4.2 Comprehension and Collection

Here are two more schemes, not part of ZFC.

Axiom (Comprehension)**.** For any φ in LST,

$$\forall a \exists b \forall x \left(x \in b \leftrightarrow x \in a \land \varphi(x) \right).$$

Very loosely, this states that you can do something like

$$\{x \in A \mid \varphi(x)\}$$

Axiom (Collection)**.** For any φ in LST,

$$\forall a \left[\forall y \in a \exists ! z \varphi(y,z) \right] \to \exists b \forall y \in \exists z \in b \varphi(y,z)$$

In other words, if φ defines a "function".

Collection is "looser" than replacement. Given a set A, replacement states that it's possible to get $f(A)$ exactly, "replacing" every element of $a \in A$ with $f(a)$. Collection only lets you collect them in a big blob.

Exercise 4.1. In ZF without replacement, Comprehension and Collection together are equivalent to replacement.

Sketch of Proof. It's easy to see Comprehension and Collection together give Replacement. Also, Replacement implies Collection. To see Replacement gives Comprehension, assume $B \neq \varnothing$ and contrive a function. $\square$

§4.3 Set abstraction and the "set of all sets"

Because Comprehension holds in ZF, we can write the shorthand

$$\{x \in a \mid \varphi(x)\}.$$

This is called a *set abstract* The condition $x \in a$ is crucial; it must be a *restricted* abstract. Otherwise everything burns.

What happens when this restriction is dropped? The resulting expression may then fail to denote a set.

Proposition 4.2

The expression $\{x \mid x = x\}$ is not a set.

Proof. Assume not, and let v denote it. Clearly $v = v$, so $v \in v$. Then

$$v \in v \in v \in \dots$$

which breaks Foundation. □

In other words, the universe $V = \{x \mid x = x\}$ is not itself a set.

The way to think of this is that "I am in this room" is not the same as "this room is contained in the physical universe". The universe is not really a container; it is a "stage" on which the actual sets lie.

Nonetheless, we will use this notation for non-sets as well. Just be careful... In the above, V is not a set, it is a class. But for example, consider the expression

$$\{z \mid \exists y \, (z \in \{y\} \land y \in a)\} .$$

This is a set by replacement; roughly, consider a function $x \mapsto \{x\}$. To write it as a restricted comprehension, we must use

$$\{z \in \mathcal{P}(a) \mid \exists y \, (z \in \{y\} \land y \in a)\} .$$

§4.4 Some abuse of notation with sets and classes

Despite the warning above, we will write

$$b \in \{x \mid \varphi(x)\}$$

which doesn't necessarily make sense, since the RHS is not really a set, but this is shorthand for $\varphi(b)$. (Note we can't replace $\in$ with $\ni$ here!)

Similarly, we may write

$$\{x \mid \varphi(x)\} = \{x \mid \psi(x)\}$$

as shorthand for

$$\forall x \, (\varphi(x) \leftrightarrow \psi(x)) .$$

Similarly,

$$\{x \mid \varphi(x)\} \subseteq \{x \mid \psi(x)\}$$

is shorthand for

$$\forall x \, (\varphi(x) \to \psi(x)) .$$

Just distinguish with sets and classes...

That means we can write the following shorthands.

- **Comprehension** states that for all sets x and classes C, $C \cap x$ is a set.
- **Replacement** states that For all sets a and all class functions F, the image $F(a)$ is a set.
- **Collection** is similar to replacement but only gives you that $F(a)$ is a subset of some set.

§4.5 Some more basic notions

4.5.1 Intersection and Difference

Definition 4.3 (Intersection)**.** Given x, we define the intersection by

$$\bigcup x = \{z \mid \forall y \in x (z \in y)\}.$$

This is a set because we can put $z \in \bigcup y$.

Definition 4.4 (Difference)**.** Given x and y, define the difference by

$$x \setminus y = \{z \in x \mid z \notin y\}.$$

4.5.2 Ordered Pairs

We would like to define ordered pairs as well; $\{x_1, x_2\} = \{x_2, x_1\}$ so we need a new notion.

Definition 4.5. Let (x_1, x_2) denote $\{x_1, \{x_1, x_2\}\}$.

Notice that $(x_1, x_2) \neq (x_2, x_1)$ if $x_1 \neq x_2$, and $(x, x) = \{\{x\}, \{x, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$.

Exercise 4.6. Show that $(x_1, x_2) = (y_1, y_2)$ if and only if $x_1 = y_1$ and $x_2 = y_2$.

4.5.3 Products

We can define the direct product.

Definition 4.7. Define

$$X \times Y = \{(x, y) \mid x \in X \wedge y \in Y\}.$$

We claim this is a set. Just notice we can carve it out from $\bigcup \mathcal{P}(\mathcal{P}(X \cup Y))$.
Naturally, we can also define

$$X_1 \times X_2 \times \cdots \times X_{n+1} = (X_1 \times \cdots \times X_n) \times X_{n+1}.$$

We also write $X^n = X \times X \times \cdots \times X$.

4.5.4 Relations

An n-ary relation R on a class X is a subclass of X^n.
Suppose $n = 2$. The domain of R is

$$\operatorname{dom}(R) = \{x \in X \mid \exists y (x \; R \; y)\}.$$

Similarly,the range is

$$\operatorname{ran}(R) = \{y \in Y \mid \exists x (x \; R \; y)\}.$$

Then we let

$$\operatorname{field}(R) = \operatorname{dom}(R) \cup \operatorname{ran}(R).$$

We can define

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}.$$

Finally, we say that R is

- *reflexive* if $\forall x \in X$, $x \; R \; x$..
- *symmetric* if $\forall x, y \in X$, $x \; R \; y \to y \; R \; x$.
- *transitive* if $\forall x, y, z \in X$ we have $x \; R \; y \land y \; R \; z \to x \; R \; z$.

It is an equivalence relation if all three are true. This gives us a partition into equivalence classes $[a]_R$.

Exercise 4.8. Show that

(i) $X = \bigcup \{[a]_R \mid x \in X\}$.

(ii) $\forall a, b \in X \, (\neg \, (a \; R \; b) \to [a]_R \cap [b]_R = \varnothing)$

4.5.5 Functions

A function is a binary relation R such that

$$\forall x \in \operatorname{dom}(R) \quad \exists! y \in \operatorname{ran}(R) : x \; R \; y.$$

We'll use f and g, thanks. Also, for sets X and Y write

$${}^X Y = \{f \mid f : X \to Y\}.$$

Thus ${}^\omega\omega$ is the functions from $\mathbb{N}$ to $\mathbb{N}$. We sometimes abuse notation if there is no possibility of confusion and write this as Y^X.

Restriction, images, inverses.

§4.6 Philosophy

Everything is a set. $\mathbb{N}$ is a set. $\mathbb{R} = \mathcal{P}(\mathbb{N})$ is a set. And so on.

OK let's move on.

§4.7 Axiom of Choice

Axiom IX (Choice)**.** We have

$$\forall x \, (\forall y \in x \, (y \neq \varnothing)) \to \exists f \, (f \text{ is a function}, \; \operatorname{dom}(f) = x, \; \forall y \in x \, (fy \in y)).$$

In other words, given a bunch of nonempty sets $x = \{y_1, y_2, \dots\}$, we can construct a choice function f with $f(y_i) \in y_i$ for all i.

Note that this can be proven in the case x is finite. Let $x = \{y_1\}$, where $y_1 \neq \varnothing$. Look at all functions f with domain x and $f(y_1) \in y_1$.

In the case $x = \{y_1, y_2\}$ with $y_1, y_2 \neq \varnothing$.

Then $y_1 \times y_2 \neq \varnothing$.

In other words, Choice states that $y_1 \times y_2 \times \dots$ is nonempty, even in the infinite case.

Exercise 4.9. Show that Choice is equivalent to

$$\forall x \forall y \forall f : x \to y \quad \exists (g : \operatorname{ran}(f) \to x) \text{ such that } g \subseteq f^{-1}.$$

§5 September 16, 2014

Summary so far:

(1) informal introduction to the subject matter of set theory

- V
- two fundamental notions: well-ordering (stages) and power sets (what we do to stages)

(2) axioms of set theory

Now, we redo our (1) formally using (2).

Recall (informally) our ordinals, $0, \dots, \varepsilon_0, \dots$. We're going to make this all rigorous now.

§5.1 Motivation

Our motivation is that we are going to try and generalize the natural numbers ω. Recall we have induction: if $\varphi(0)$ and $\forall n\,(\varphi(n) \to \varphi(n+1))$ then $\forall n \varphi(n)$. This is not enough to get up to ω. Now we're going to generalize this massively a la "strong induction".

We are also going to generalize recursion. Given a point p, if we can get $f(p)$ from all predecessors of p, then we have a recursion.

We're going to do this vastly more generally, on well-founded rather than just well-ordered relations.

§5.2 Setup

Let R be a binary relation on X.

Definition 5.1. We say R is **strict** or irreflexive if $\forall x \in X$, $x\ R\ x$ does NOT hold. We say R is **linear** if $\forall x, y \in X$ either $x\ R\ y$ or $y\ R\ x$.

Then for each $x \in X$, let

$$\operatorname{ext}_R(x) = \{y \in X \mid y\ R\ x\}.$$

Example 5.2

Let R denote "is a parent of" and X be the set of humans. Then R is strict but not linear. Moreover, $\operatorname{ext}_R(x)$ are the parents of x.

Definition 5.3. The **transitive closure** $\operatorname{TC}(R)$ is the intersection of all transitive relations containing R.

By taking the intersection of them all, we get rid of the "junk" and get the smallest possible.

Example 5.4

$\operatorname{TC}(\text{"is a parent of "}) = \text{"is an ancestor of"}$.

Definition 5.5. The **predecessors** are $\operatorname{pred}_R(x) = \operatorname{ext}_{\operatorname{TC}(R)}(x)$. A subset Y of X is R-transitive if for all $y \in Y$, $\operatorname{pred}_R(y) \subseteq Y$.

Example 5.6
The set $\text{pred}_R(\text{Fred Koellner}) \cup \text{pred}_R(\text{Obama})$ is R-transitive.

Definition 5.7. An element $y \in Y$ is **R-minimal** if there is no $z \in Y$ such that $z \neq y$ and $z \; R \; y$.

Then a relation R (on X, even if it is a class rather than a set) is **well-founded** if

(i) Every nonempty subset Y has an R-minimal element

(ii) $\forall x \in X$, $\text{ext}_R(x)$ is a set.

Note that this last relation is obvious for X a set. However, we can consider X a class as well, so long as locally everything looks like a set (for example, "set of all sets").

Definition 5.8. A **well-ordering** is a well-founded, strict, linear relation.

§5.3 Transfinite Induction

Now we can generalize induction and recursion to well-founded relations. (If you look at the proof of induction, neither "linear" nor "countable" is needed.)

Theorem 5.9 (Transfinite Induction)
Suppose R is a well-founded relation on X. If $Y \subseteq X$ is such that

$$\forall x \in X \; (\text{pred}_R(x) \subseteq Y \to x \in Y)$$

then $Y = X$.

In other words, let Y be some subset of X. Suppose that any time the predecessors of x are in Y, then x is in Y too. It follows that, actually, all of X is in Y.

The "base cases" are handled by $\text{pred}_R(x) = \varnothing$ for any R-minimal element x.

Proof. Suppose that $Y \neq X$ and consider $X - Y$. Then let a be an R-minimal element in $X - Y$. Now all the guys in $\text{pred}_R(a)$ cannot be in $X - Y$, so they are contained in Y. Contradiction. $\square$

§5.4 Transfinite Recursion

Likewise, we can also build objects on well-founded structures.

Theorem 5.10 (Transfinite Recursion)
Suppose R is a well-founded relation on X. Suppose

$$G : X \times V \to V$$

is a class function. Then there's a unique function

$$F : X \to V$$

so that for all $x \in X$,

$$F(x) = G(x, F|_{\text{pred}_R(x)}).$$

Here $F|_{\text{pred}_R(x)}$ is a restriction.

Here G is a "generating function" in the sense of the recursion. Our G takes in an x and the predecessors, and spits out $F(x)$. Intuitively, G has way, way more information than we need.

Proof. First, we show uniqueness. Suppose F_1 and F_2 are two distinct such functions. Use transfinite induction to show they are equal: consider the R-minimal point a with $F_1(a) \neq F_2(a)$. Then $F_1|_{\text{pred}_R(a)} = F_2|_{\text{pred}_R(a)}$, contradicting that G is a function.

For existence, take an R-minimal element x. Our G gives $G(x, \varnothing)$, so now we know $F(x)$. Intuitively, it's clear how to proceed.

Let us say a function $f : D \to V$ is **good** if

(i) $D \subseteq X$ and $\forall x \in D(\text{pred}_R(x) \subseteq D)$

(ii) $\forall x \in D$ we have $f(x) = G(x, f|_{\text{pred}(x)})$.

In other words, f is doing the right thing on a predecessor-closed subset of X.

First, suppose $f_1 : D_1 \to V$ and $f_2 : D_2 \to V$. We claim $f_1|_{D_1 \cap D_2} = f_2|_{D_1 \cap d_2}$. The proof is exactly the same as that for uniqueness.

The second claim is that

$$\bigcup \{\text{dom}(P) \mid f \text{ is good}\}$$

is X. Now suppose $f : \text{pred}_R(x) \to V$ is good for some x. Define $f' : \text{pred}_R(x) \cup \{x\} \to V$ by

$$y \mapsto \begin{cases} f(y) & \text{if } y \in \text{pred}_R(x) \\ G(x, f) & \text{otherwise.} \end{cases}$$

This is clearly good. So we have shown that

$$\text{pred}_R(x) \subseteq \bigcup \{\text{dom}(f) \mid f \text{ is good}\} \to x \in \bigcup \{\text{dom}(f) \mid f \text{ is good}\}.$$

The second claim then follows by transfinite induction.

Finally, let $F = \bigcup \{f \mid f \text{ good}\}$. By Claim 1 this is a function. By Claim 2, $\text{dom}(F) = X$. Hence F is good. $\square$

§5.5 Transfinite things can be BIG

Let $G : V \times V \to V$, and let R be the membership relation $\in$. For any set x, we have

$$\text{ext}_\in(x) = x.$$

Then $\text{pred}_\in(x)$ consists of a very nested sequence of things. In particular, $\varnothing \in \text{pred}_\in(x)$. It really goes ALL THE WAY DOWN.

A second example is

$$G : \text{On} \times V \to V \text{ by } (\alpha, f) \mapsto \begin{cases} \mathcal{P}\left(\bigcup \text{ran}(f)\right) & \text{if } \alpha \neq \varnothing \\ \varnothing & \text{otherwise.} \end{cases}$$

with R as $<$. The transitive recursion gives us an F such that for any $\alpha \in \text{On}$ we have

$$F(\alpha) = G(\alpha, F_\alpha)$$

and you can check that in fact,

$$F(0) = F(\varnothing) = G(\varnothing, \varnothing) = \varnothing = V_0.$$

Oops okay this doesn't actually work. OK, the correct version is

$$G : \mathrm{On} \times V \to V \text{ by } (\alpha, f) \mapsto \begin{cases} \varnothing & \text{if } \alpha = \varnothing \\ \mathcal{P}(\bigcup \mathrm{ran}(x)) & \text{if } \alpha \text{ is a successor} \\ \bigcup \mathrm{ran}(x) & \text{if } \alpha \text{ is a limit.} \end{cases}$$

§6 September 18, 2014

Last time we looked at transfinite induction as well-founded relations.

Basically, a well-founded relation (X, R) is just one step shy of being a sub-chunk of the ordinals. A well-founded relation looks a lot like a poset with a base. You can have infinite ascending sequences, just not descending ones (limit points).

A special case is a well-orderings. The main topic for today.

§6.1 What does a well-ordering look like?

Imagine a poset with a base in which every two things are comparable. Oh wait, we have a total order.

We can also add limit points.

Anyways, the basic claim is that any well-ordering is just isomorphic to sub-orderings of the standard ordering of the ordinals.

§6.2 Well-orderings look roughly the same

Definition 6.1. Suppose (X, R) is a well-ordering. For $x \in X$, we define another well-ordering

$$I_x^R = \left(\text{pred}_R(x), R \cap \text{pred}_R(x)^2\right).$$

Here I_x^R and R itself are called the **initial segments** of (R, X).

Intuitively, all we're doing is cutting off our relation past x.

Remark. A different notation of a well-ordering is $(A, <_A)$. We sometimes also abbreviate (X, R) as just R.

The following proof is just a generalization of the proof that the natural numbers are unique up to isomorphism. First, let us make sure we agree on the definition of isomorphism:

Definition 6.2. Suppose (X, R) and (X', R') are well-orderings. We say that $(X, R) \cong (X', R')$ are isomorphic if f is bijective.

Remark. We can weaken "bijective" to "surjective" because R' is strict and R is linear. Explicitly, if $x_1 \neq x_2$, then they are R-related, so fx_1 and fx_2 are R-related and hence not equal.

Theorem 6.3

Suppose (X, R) and (Y, S) are well-orderings. Then either

(i) $R \cong I_y^S$ for some $y \in Y$,

(ii) $I_x^R \cong S$ for some $x \in X$,

(iii) $R \cong S$.

Again, the proof is just to walk upwards.

Proof. For $A \subseteq X$, $f : A \to Y$ and $x \in X$. We use transfinite recursion. Let

$$G(x, f) = \begin{cases} s\text{-least element in } Y - f(\text{pred}_R(x)) & \text{if possible} \\ \text{undefined} & \text{otherwise.} \end{cases}.$$

OK this is pretty sloppy. But lol. We're allowed to be sloppy because in set theory, functions are just pairs, and so "undefined" means we just don't add a pair. But consequently, G might not have the full domain X.

But the point is that if we exhaust S, then we're done, and if we haven't run out of things in S, we just keep going.

Let F be defined by transfinite recursion from G. By transfinite induction we have

$$\forall x \in \text{dom}(F) F\left(\text{pred}_R(x)\right) = \text{pred}_S\left(F(x)\right).$$

Also it's easy to see F is order-preserving (both ways). Blah.

OK we finish by considering three cases.

(1) If $\text{dom}(F) = X$ and $\text{ran}(F) = Y$, then $R \cong S$.

(2) If $\text{dom}(F) = X$ and $\text{ran}(F) \neq Y$, then just take the minimal element y of $Y - \text{ran}(F)$, then this must be equal to $\text{pred}_S(y)$, thus $R \cong I_y^S$.

(3) The case $\text{dom}(F) \neq X$ is handle similarly and we obtain $R \cong I_x^R$. ☐

§6.3 Stuff with classes

For a given well-ordering (X, R) consider the *class* of all well-orderings $(X1, R')$ such that

$$(X', R') \cong (X, R).$$

This gives a massive equivalence class.

Example 6.4

The equivalence class of $(\omega, \in)$ has a lot of things. For example, consider $(\text{Even}, <)$, $(\text{Odd}, <)$. This is not even a set. Given S, we can construct a copy of ω by putting $\in$ on

$$S, \{S\}, \{\{S\}\}, \ldots$$

and things blow up!

Also the equivalence classes are stacked too. For C_1 and C_2 are equivalence classes of a well-ordering. Pick $(x_1, R_1) \in C_1$ or $(X_2, R_2) \in C_2$. WLOG, assume R_1 is an initial segment of R_2. Then every guy in C_1 is an initial segment of C_2. That means the equivalence classes are well-ordered too.

Now we want to pick a specific canonical representative from each equivalence class. Here's how you do it. Given (X, R) a representative of a class, we want to add a single element. There are tons of elements not in X, but the canonical one is X. Hence we do

$$X' = X \cup \{X\}$$

and

$$R' = R \cup \{(y, X) \mid y \in X\}.$$

So starting with the empty set, we have a trivial relation $(\varnothing, \varnothing)$, and we recover the ordinals.

§6.4 How to preserve transitive sets

Recall that a set A is transitive if $a \in A \implies a \subseteq A$.

Lemma 6.5

If X is transitive then

(a) $X \cup \{X\}$ is transitive

(b) $\cup X$ is transitive

(c) $\mathcal{P}(X)$ is transitive.

Proof. (a) Consider $x \in X$ and do cases on $x \in X$ versus $x = X$.

(b) Suppose X is transitive. Then $\cup X$ is transitive. Suppose $a \in \cup X$. Then $a \in b \in X$ for some b. By transitivity, $a \in X$, and hence by union $a \subseteq \cup X$.

(c) Check it. □

Of course, $\varnothing$ is transitive. So V_α are all transitive by invoking the lemma. The stem On consists of transitive sets too.

§6.5 Ordinals

Definition 6.6. An **ordinal** is a transitive set that is well-ordered by $\in$.

Let On denote the class of ordinals.

Every transitive set is closed under membership $\in$. Ordinals are additionally well-ordered under $\in$.

You can show that any transitive well-ordering is isomorphic to some ordinal.

Exercise 6.7. If $\alpha \in \mathrm{On}$ and $\beta \in \alpha$ then $\beta \in \mathrm{On}$.

Proof. To show β is transitive, use both the fact that α is transitive and well-ordered. (Neither alone is sufficient.)

To show that β is well-ordered by $\in$, then... □

Exercise 6.8. If $\alpha \in \mathrm{On}$ then

$$\alpha = \{\beta \mid \beta < \alpha\}.$$

Here $<$ means $\in$.

Lemma 6.9

Suppose $\alpha \in \beta \in \mathrm{On}$. The following are equivalent. Then $\alpha \in \beta$ if and only if $\alpha \subsetneq \beta$.

Proof. Clearly $\alpha \in \beta \implies \alpha \subseteq \beta$, and $\alpha \neq \beta$ is not possible (since otherwise $\beta \in \beta$). The reverse is more tricky.

Now suppose $\alpha \subsetneq \beta$. Since β is well-ordered under membership, we can consider an $\in$-least element b in $\beta - \alpha$. By the first exercise, $b \in \mathrm{On}$. By the second exercise, $b = \{\gamma \mid \gamma < b\} = \alpha$. So $\alpha \in \beta$. □

Theorem 6.10 (Linearity)

If α and β are ordinals then either $\alpha \le \beta$ or $\beta \le \alpha$.

Proof. Check $\alpha \cap \beta \in \mathrm{On}$. We claim that $\alpha \cap \beta$ is either α or β. If not, $\alpha \cap \beta \subsetneq \alpha, \beta$. By the lemma, $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$. Hence $\alpha \cap \beta \in \alpha \cap \beta$ and that is a contradiction. $\square$

Theorem 6.11

On is not a set.

Proof. Assume Ω is the set of all ordinals. Then Ω is well-ordered by $\in$. Moreover, if $a \in b \in \Omega$, then b is an ordinal, so a is on ordinal, hence Ω is transitive. $\square$

§7 September 23, 2014

§7.1 Recap

- Well-orderings and well-founded relations
- Transfinite induction
- Transfinite reduction
- Well-ordering theorems – isomorphism.
- On is not an ordinal (not a set)

Recall that an ordinal is a transitive set which is well-ordered by the relation $\in$.

§7.2 Order Types

We will now show that ordinals are indeed a canonical representative.

Theorem 7.1 (Comprehensiveness)
Fro every well-ordering (X, R) there is an ordinal α such that

$$(X, R) \cong (\alpha, \in).$$

This proof is a little subtle. Actually, Schimmerling does not give a full proof.

Proof. Fix a well-ordering (X, R).

Claim. For any $a \in X$ there is a unique ordinal α with $I_a^R \cong (\alpha, \in)$.

Proof of lemma. First, we prove existence. Take the R-minimal one $a \in X$. Then look at the things below it:

$$\forall \overline{a} \in X \left(\overline{a} R a \to \exists! \overline{x} \in \text{On } I^R \overline{a} \cong (\overline{\alpha}, \in) \right).$$

Now pick using Replacement

$$\alpha = \left\{ \alpha \mid \exists \overline{a} R a \; I_{\overline{a}}^R \cong (\alpha, \in) \right\}.$$

To prove α is an ordinal, it suffices to prove that it is is transitive (since it is clearly well-ordered by $\in$). You can check this. Fix $\overline{\overline{\alpha}} \in \overline{\alpha} \in \alpha$. Then $\overline{\alpha}$ has an $\overline{a} \in I_{\overline{a}}^R \cong (\overline{\alpha}, \in)$. Now $\overline{\overline{\alpha}} \in (\overline{\alpha}, \in)$, so $\overline{\overline{a}} \in I_{\overline{a}}^R$. That gives $\overline{\overline{\alpha}} \in \alpha$.

Hence there exists such an α with

$$I_a^R \cong (\alpha, \in).$$

Of course, this α is unique, since

$$(\alpha, \in) \cong I_a^R \cong \left(\alpha', \in\right)$$

implies $\alpha \cong \alpha'$. ■

Hence, for any initial segment in (X, R) we can get a corresponding ordinal. Now to hit all of (X, R) we can set

$$\beta = \left\{ \overline{\beta} \mid \exists \overline{a} \in X I_{\overline{a}}^R \cong (\overline{\beta}, \in) \right\}.$$ □

Definition 7.2. Suppose (X, R) is a well-ordering. Then the order type of (X, R) is the unique ordinal α such that $(X, R) \cong (\alpha, \in)$.

Exercise 7.3. Show that there are arbitrarily large limit ordinals.

This is not true without Replacement, since $V_{\omega+\omega}$ is a model of ZFC minus Replacement. You need Replacement to show that $\lambda + \omega$ is a set for any limit ordinal λ.

§7.3 Arithmetic on Ordinals

There are two approaches,

- transfinite induction,
- explicit construction.

We want to get $\alpha + \beta$, $\alpha \cdot \beta$, α^β.

7.3.1 Addition

The transfinite recursion method is as follows.

$$\begin{aligned} \alpha + 0 &= \alpha \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1 \\ \alpha + \lambda &= \bigcup_{\beta < \lambda} (\alpha + \beta). \end{aligned}$$

Here $\lambda \neq 0$.

For explicit construction, we work by concatenation. Suppose we have (X, R), (Y, S) (so we do this with any well-orderings rather than just with ordinals, even though it's the same concept.). Basically we want to stick Y on top of X, so we do a quick hack by using ordered pairs. Define

$$(X, R) + (Y, S) = \left((\{0\} \times X) \cup (\{1\} \times Y), <_{\text{lex}} \right)$$

Yay. Since we can add well-orderings, we can add ordinals by just looking at order types.

It is not too hard to check that these definitions coincide (just use transfinite induction).

Example 7.4

Note that $2014 + \omega = \omega \neq \omega + 2014$.

Remark 7.5. Ordinal addition is not commutative. However, it is associative.

7.3.2 Multiplication

Again, it suffices to define things using transfinite recursion.

$$\begin{aligned} \alpha \cdot 0 &= \alpha \\ \alpha \cdot (\beta + 1) &= (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \lambda &= \bigcup_{\beta < \lambda} \alpha \cdot \beta. \end{aligned}$$

We can also do explicit construction.

$$\alpha \cdot \beta = \left(\beta \times \alpha, <_{\text{lex}} \right).$$

Again transfinite induction lets you show these are the same.

Example 7.6

Check that $2014 \cdot \omega = \omega \neq \omega \cdot 2014$ for similar reasons as addition.

Remark 7.7. Like addition, multiplication is associative (since we just get ordered triples in the second definition), but not commutative.

7.3.3 Exponentiation

The recursion is clear.

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^{\beta+1} &= \alpha^\beta \cdot \alpha \\ \alpha^\lambda &= \bigcup_{\beta<\lambda} \alpha^\beta. \end{aligned}$$

The explicit construction is more complicated here, so tl;dr, have fun with the exercises.

7.3.4 A nontrivial theorem

Exercise 7.8 (Division Algorithm)**.** Suppose we have a "base" ordinal $\beta > 0$. Let α be an ordinal. Then there exists a unique choice of γ_1, γ_2 such that

$$\alpha = \beta \cdot \gamma_1 + \gamma_2$$

and $\gamma_2 < \beta$.

Proof. Mimic the proof of the division algorithm. □

Theorem 7.9 (Cantor Normal Form)

Suppose $\alpha > 0$ is an ordinal. Then α can be written uniquely as

$$\alpha = \omega^{\beta_1} \cdot \kappa_1 + \omega^{\beta_2} \cdot \kappa_2 + \cdots + \omega^{\beta_n} \cdot \kappa_n$$

where $\alpha > \beta_1 > \cdots > \beta_n \geq 0$ are ordinals, and $\kappa_1, \dots, \kappa_n, n$ are positive integers.

Proof. Transfinite induction. Just greedily do it. LOL. □

§7.4 The hierarchy of sets, done with ordinals

Definition 7.10. By transfinite induction, we set

$$\begin{aligned} V_0 &= \varnothing \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\lambda &= \bigcup_{\alpha<\lambda} V_\alpha \end{aligned}$$

Finally, let V be the following class.

$$V = \bigcup_{\alpha \in \mathrm{On}} V_\alpha.$$

This is the "cumulative hierarchy of sets".

Lemma 7.11

For all $\alpha, \beta \in \mathrm{On}$ such that $\alpha < \beta$,

(1) V_α is transitive,

(2) $V_\alpha \subseteq V_\beta$.

Proof. The proof of (1) is just transfinite induction on α. For (ii), $V_\alpha \in V_\beta \implies V_\alpha \subseteq V_\beta$. (The first part is just mass power set.) $\square$

§7.5 The ordinals grab all the sets

Exercise 7.12. Show that

$$\{x \mid x = x\} = V \overset{\text{def}}{=} \bigcup_{\alpha \in \mathrm{On}} V_\alpha$$

In other words, every set is picked up in $\bigcup_{\alpha \in \mathrm{On}} (V_\alpha)$.

Proof. If some set doesn't appear, take an $\in$-minimal set not in any ordinal (possible since Foundation tells us $\in$ is well-founded). Thus the key is Foundation. $\square$

The exercise implies the following notion is well-defined.

Definition 7.13. The rank of a set x, written $\mathrm{rank}(x)$, is the least α such that $x \in V_{\alpha+1}$.

Remark 7.14. Notice that $\mathrm{rank}(\alpha) = \alpha$ and $\mathrm{rank}(V_\alpha) = \alpha$ for every $\alpha \in \mathrm{On}$.

Here is an alternative definition.

Definition 7.15. Show that an equivalent definition is as follows. By transfinite recursion on $(V, \in)$, we define for each $x \in V$ with $x \neq \varnothing$ by

$$\begin{aligned} \rho(\varnothing) &= 0 \\ \rho(x) &= \bigcup_{y \in x} (\rho(y) + 1) \end{aligned}$$

Remark 7.16. This is why we want to have transfinite recursion on well-founded structures, not just well-orderings.

Exercise 7.17. Show that rank and ρ coincide.

§8 September 25

Today we discuss cardinals. In ordinals, order matters; it doesn't for cardinals. Note that ordinals and cardinals coincide in the finite case.

Ordinals are a canonical representative for well-orderings. The idea is to do the same thing with equivalence classes of bijections: we want to pick a canonical representative for each of these guys.

At the end of this lecture, we state CH and then shoot for it.

§8.1 Axiom of Choice is equivalent to WO

Recall that our axiom states that there exists a choice function for any collection of sets X.

Cantor implicitly assumes that every set can be well-ordered. (Can $\mathbb{R}$ be well-ordered?) This isn't quite true.

Theorem 8.1 (Zermelo, 1904)
The following are equivalent.

(1) AC, the Axiom of Choice.

(2) WO, which states that every set X can be well-ordered.

Proof. First, let us show that AC implies WO. Let X be an arbitrary set. Pick a choice function f on $\mathcal{P}(X) - \{\varnothing\}$ (this follows from AC). Hence every subset $Y \subseteq X$ has a choice $f(y) \in X$.

First, pick $x_1 = f(X) \in X$. Now we have a first element. Select $x_2 = f(X - x_1) \in X - x_1$, and so on. In general, we wish to define $f^* : \beta \to X$ such that for each $\alpha < \beta$,

$$f^*(\alpha) = f(X) - \bigcup_{x \in \alpha} f^*(x).$$

This process cannot continue forever, since otherwise X is bijected to the ordinals, which is impossible (recall that X is a set). Hence we can find β as above, so we have a well-ordering of X, namely β.

Now assume WO; we wish to show AC. Let X be an arbitrary set whose elements are not $\varnothing$. Now take a well-ordering R on $\bigcup X$. Then given any set $Y \in X$, we just the R-minimal element. ☐

Yeah OK so AC is equivalent to the assertion that everything is well-ordered. GG.

§8.2 Zorn's Lemma

Definition 8.2. Let $(X, \trianglelefteq_X)$ be a **poset** or partial ordering; i.e. a reflexive transitive relation on the set X An element of $x \in X$ is **maximal** if

$$\nexists x' \in X \left(x \triangleleft x'. \right)$$

Definition 8.3. A subset $C \subseteq X$ is a **chain** if C is linearly ordered by $\trianglelefteq_X$. An element is $x \in X$ is an **upper bound** for a chain C if $\forall c \in C$, $c \trianglelefteq_X x$.

Remark. Note that this upper bound does *not* nead to lie in C.

Definition 8.4 (Zorn's Principle)**.** If $(X, \leq_X)$ is a partial ordering such that every chain has an upper bound then $(X, \trianglelefteq_X)$ has a maximal element.

Theorem 8.5 (Zorn's Lemma)

AC is equivalent to Zorn's Principle.

Proof. Assume AC and WO. We wish to show ZP. Let $(X, \trianglelefteq_X)$ be a partial order such that all chains have an upper bound.

By WO we can put a well-order $\prec$ with order type β on X. Pick first the $\prec$-minimal point $x_0 = f(0)$. Then let x_1 be the $\prec$-least point above x_0. Repeat for the successors (we're using our contradiction assumption). Then we'll set x_ω to be the $\prec$-least z above the chain $x_0 \triangleleft x_1 \triangleleft x_2 \triangleleft \dots$. In general set x_λ to be the $\prec$-least number above x_α for every $\alpha < \lambda$. This process must terminate eventually, since the resulting chain C can be embedded in β. It can only terminate when we have reached a maximal element.

Now to show that ZP implies AC. Look at the set of partial choice functions $\mathcal{P}$, ordered by $\trianglelefteq_P$ be the poset of partial choice functions on X "ordered by extension"; i.e.

$$P = \left\{ f : \overline{X} \to \bigcup \overline{X} \text{ is a choice function} \mid \overline{X} \neq \varnothing \text{ and } \overline{X} \subseteq X \right\}.$$

The order is just $f \trianglelefteq_P g$ if and only if $f \subseteq g$ (not $\operatorname{dom} f \subseteq \operatorname{dom} g$!). Observe that for any chain C, the function $\bigcup C$ is an upper bound for the chain C. By Zorn, we now have a maximal element in P, denoted F. It follows that F is the required choice function, because the only possible maximal elements of F are complete choice functions. $\square$

Moral: partial orders should approximate the order that you want
Reverse mathematics: our lemmas prove the axioms.

§8.3 Some weakenings of AC

Definition 8.6 (Dependent Choice, DC)**.** Given a relation $\sim$ such that for every x there is something related to it, we can construct a chain $\{x_i : i < \omega\}$ such that for all $i < w$, we have

$$x_i \sim x_{i+1}.$$

This is called "dependent" since previous steps matter for future steps.

Exercise 8.7. Show that AC implies DC.

Fact 8.8. DC does not imply AC.

Definition 8.9. A set X is countable if and only if X can be bijected to ω.

Definition 8.10 (Countable Choice, AC_ω)**.** Every countable set of nonempty sets has a choice function.

Exercise 8.11. Show that DC implies AC_ω.

Fact 8.12. AC_ω does not imply DC.

§9 September 30, 2014

Last time we showed AC, WO, and Zorn are equivalent.

In what follows, AC is not assumed until further notice.

§9.1 Equinumerous sets

The following definition is actually really important; historically, it was not recognized as significant.

Definition 9.1. Two sets A and B are **equinumerous**, written $A \approx B$, if there is a bijection between them.

Definition 9.2. We say $A \preceq B$ if we can injection A into B.

Clearly, $\mathbb{N} \preceq \mathbb{Q} \preceq \mathbb{R}$, and $\mathbb{N} \approx \mathbb{Q} \not\approx \mathbb{R}$.

Example 9.3

Set $E = \{0, 2, 4, \dots\}$ and $O = \{1, 3, 5, \dots\}$. Then $E \approx \mathbb{N} \approx O$.

Example 9.4

$\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

The following fundamental theorem shows that this notation makes sense.

Theorem 9.5 (Cantor-Bernstein)

Suppose $A \preceq B$ and $B \preceq A$. Then $A \approx B$.

Proof. We are given injective functions $f : A \to B$ and $g : B \to A$ and desire a bijection $h : A \to B$.

Define $X_0 = A$, $Y_0 = B$, and recursively set

$$X_{n+1} = g(Y_n) \text{ and } Y_{n+1} = f(X_n).$$

This gives us a set of chains

$$X_0 \supseteq X_1 \supseteq X_2 \supseteq \dots$$

and similarly for Y. Let $X^\infty = \bigcap_{n \in \mathbb{N}} X_n$. Define now $h : A \to B$ by

$$x \mapsto \begin{cases} f(x) & \text{if } x \in X_n \setminus X_{n+1} \text{ for some even } n \\ g^{-1}(x) & \text{if } x \in X_n \setminus X_{n+1} \text{ for some odd } n \\ f(x) & \text{if } x \in X^\infty. \end{cases}$$

The point is that $f(X^\infty) = g^{-1}(X^\infty) = Y^\infty$, so in the last sentence we could replace f with g^{-1} (this would lead to a different h, but both are still bijections).

Check that this works. $\square$

§9.2 Creating cardinals

Definition 9.6. A **cardinal** is an ordinal κ such that for no $\alpha < \kappa$ do we have $\alpha \approx \kappa$.

Remark 9.7. These are also called *initial ordinals*.

You can check that all the ordinals $\omega + \omega$, ω^2, ω^ω, and even ϵ_0 are all countable sets, so none of them are cardinals.

Remark 9.8. The first few cardinals are 0, 1, ... Then, ω is a cardinal as well, and we set $\aleph_0 = \omega$.

Our goal is to prove the following proposition.

Proposition 9.9
There are arbitrarily large cardinals.

If we had WO (equivalently AC) right now, for X we could define

$$|X| = \text{least ordinal } \kappa \text{ with } X \approx \kappa.$$

This must be a cardinal, by definition. (The *existence* of such a κ is equivalent to WO. In fact, AC is equivalent to every set having a cardinality.) Now we could construct a cardinal greater than ω by taking $|\mathcal{P}(\omega)|$, which is a cardinal.

However, one can show this without WO.

Exercise 9.10. Given an ordinal κ, let κ^+ be the least ordinal cardinal greater than κ. Show that κ^+ exists.

Sketch. Take the supremum of all the guys that have a $1-1$ correspondence with κ. Show that the guys form a set. Use Replacement? □

This shows that the class of cardinals $\mathcal{C}$ is not a set. For otherwise, $\cup\mathcal{C}$ has a cardinality κ, but there's a cardinal greater than κ in $\mathcal{C}$.

§9.3 Properties of cardinals

Lemma 9.11
Given any set A of cardinals, $\bigcup A$ is a cardinal.

This can let us construct $\aleph_\omega$.

Proof. If A has a maximal element κ, then $\bigcup A = \kappa$ and we're done.

Now suppose there is no largest cardinal. Suppose for contradiction that $\exists \alpha < \bigcup A$ which can be bijected to it by some function f. So let $\kappa \in \bigcup A$ be such that $\alpha < \kappa$. Then κ can be injected to α by restricting f, contradiction. □

Corollary 9.12
$\aleph_\omega$ exists.

Proof. Set $A = \{\aleph_0, \aleph_1, \dots\}$, and note that A is a set by Replacement. Now apply the above lemma. □

§9.4 Recurse

Summary: given a cardinal κ we can construct κ^+ a "successor" cardinal, and given a set of cardinals A we have $\bigcup A$ is a cardinal.

Hence by transfinite recursion we can define the following.

Definition 9.13. For any $\alpha \in \mathrm{On}$, we may define

$$\begin{aligned} \aleph_0 &= \omega \\ \aleph_{\alpha+1} &= (\aleph_\alpha)^+ \\ \aleph_\lambda &= \bigcup_{\alpha<\lambda} \aleph_\alpha. \end{aligned}$$

Example 9.14

Here are some big ordinals.

$$\aleph_\omega, \aleph_{\epsilon_0}$$

and

$$\aleph_{\aleph_\omega}, \aleph_{\aleph_{\aleph_\omega}}, \dots$$

If we take this to the limit, we get a κ such that $\aleph_\kappa = \kappa$. This is called an "$\aleph$-fixed point".

It's interesting to note that looking at the first few cardinals $\aleph_0$, $\aleph_1$, ..., it seems that the cardinal is much bigger than its index. Evidently, the κ mentioned above is the union of $\aleph_{\aleph_{\aleph_{\dots}}}$, where we have n $\aleph$'s.

Then we can take κ^+, ...

So now we have even showed there are arbitrarily large $\aleph$-fixed points, say κ_0, κ_1, ...

Lemma 9.15

If κ is a cardinal then either κ is finite (i.e. $\kappa \in \omega$) or $\kappa = \aleph_\alpha$ for some $\alpha \in \mathrm{On}$.

Proof. Assume κ is infinite. Take α minimal with $\aleph_\alpha \geq \kappa$. For contradiction suppose $\aleph_\alpha > \kappa$.

Now, consider two cases. If α is a limit ordinal λ, then $\aleph_\lambda$ is the supremum $\bigcup_{\gamma<\lambda} \aleph_\gamma$. So some $\gamma < \lambda$ has $\aleph_\gamma > \kappa$.

On the other hand, suppose $\alpha = \overline{\alpha} + 1$. Then

$$\aleph_{\bar{\alpha}} < \kappa < \aleph_\alpha$$

are three cardinals. This is a contradiction. ∎

Remark 9.16. Still no AC!

The Continuum Hypothesis (CH) says that if $X \subset \mathcal{P}(\omega)$ is infinite, then either $X \approx \omega$ or $X \approx \mathcal{P}(\omega)$. Given AC, we can talk about $|\mathbb{R}|$, in which case CH states $|\mathbb{R}| = \aleph_1$.

§10 October 2, 2014

More on cardinals.

§10.1 Cardinal arithmetic

Recall the way we set up ordinal arithmetic. Note that in particular, $\omega + \omega > \omega$ and $\omega^2 > \omega$.

But cardinals count cardinality. We want to have

$$\aleph_0 + \aleph_0 = \aleph_0$$
$$\aleph_0 \times \aleph_0 = \aleph_0$$

because $\omega + \omega$ and $\omega \cdot \omega$ are countable. In the case of cardinals, we simply "ignore order".

The following definition uses the Axiom of Choice.

Definition 10.1. The cardinality $|X|$ of a set X is the least ordinal α such that $|X| \approx \alpha$.

Recall that $\approx$ means "equinumerous", and this is well-defined. (AC implies that X has a well-ordering, so there is at least one such ordinal).

Definition 10.2 (Cardinal Arithmetic)**.** Given cardinals κ and λ, define

$$\kappa + \lambda = |(\{0\} \times \kappa) \cup (\{1\} \times \lambda)|$$

and

$$k \times \lambda = |\lambda \times \kappa| .$$

§10.2 Finite sets

Definition 10.3. A set X is

- **finite** if $|X| < \omega$.
- **countable** if $|X| \le \omega$.
- **uncountable** if $|X| > \omega$.

Here are two nice characterizations of finite-ness.

Definition 10.4. A set is **Dedekind-finite** (abbreviated D-finite) if every injective function from X to itself is also surjective.

Exercise 10.5. Show that a set is finite if and only if it is Dedekind finite.

Definition 10.6. A set X is **D^*-finite** if there exists $f : X \to X$ such that for no subset $\varnothing \subsetneq Y \subsetneq X$ is f closed under Y (meaning $f(Y) \subseteq Y$).

Exercise 10.7. Show that this is also a characterization of finite sets.

Partial Proof. Look at

$$\{a, f(a), f^2(a), \dots\}$$

and let this be Y. If Y is finite done. Otherwise take $Y - a$. □

Without AC you can find models of set theory for which the above equivalences break.

§10.3 Infinite cardinal arithmetic is boring

For finite cardinals, we can show that

$$n \times m > n + m > n, m.$$

But now we have the following property of cardinal arithmetic.

Theorem 10.8

Let κ be an infinite cardinal. Then $\kappa \times \kappa = \kappa$.

Proof. By transfinite induction (which is fine because we are working over ordinals), we may assume that the theorem holds for all infinite cardinals $\overline{\kappa} < \kappa$. Put an ordering on $\kappa \times \kappa$ as follows: for (α, β) and (γ, δ) in $\kappa \times \kappa$ set $(\alpha, \beta) \lhd (\gamma, \delta)$ if and only if $\max(\alpha, \beta) < \max(\gamma, \delta)$ or the maximums are equal and $(\alpha, \beta) <_{\text{lex}} (\gamma, \delta)$. (This gives a "diagonal" argument.)

We claim that the order type of $(\kappa \times \kappa, \lhd)$ equals κ.

Count the $\lhd$-predecessors of some $(\alpha, \beta) \in \kappa \times \kappa$. We claim there are at most

$$|(\max(\alpha, \beta) + 1) \times (\max(\alpha, \beta) + 1)|$$

such points. Set $\overline{\kappa} = |\max(\alpha, \beta) + 1| < \kappa$. By induction, $|\overline{\kappa} \times \overline{\kappa}| = \overline{\kappa}$.

Hence we've shown that there are at most κ points $\lhd$-below any pair, which implies that $\operatorname{ot}(\kappa \times \kappa, \lhd) = \kappa$. $\square$

Corollary 10.9

Given cardinals κ and λ, one of which is infinite, we have

$$\kappa \times \lambda = \kappa + \lambda = \max(\kappa, \lambda).$$

Proof. Compute

$$\begin{aligned} \max(\kappa, \lambda) &\le \kappa + \lambda \\ &\le \kappa \times \lambda \\ &\le \max(\kappa, \lambda) \times \max(\kappa, \lambda) \\ &= \max(\kappa, \lambda). \end{aligned}$$

$\square$

§10.4 Cardinal exponentiation

Unlike in addition and multiplication, we do not ignore order for exponentiation.

Definition 10.10. Suppose κ and λ are cardinals. Then

$$\kappa^\lambda = |\mathscr{F}(\lambda, \kappa)|.$$

Here $\mathscr{F}(A, B)$ is the set of functions from A to B.

Example 10.11

$2^{\aleph_0}$ gives us binary numbers, $\mathbb{R}$.

Continuum Hypothesis states that $2^{\aleph_0} = \aleph_1$.

§10.5 Fundamental theorems of cardinal arithmetic

Theorem 10.12 (Cantor)
For all κ, $\kappa^\kappa > \kappa$.

Proof. We already have seen (from Cantor) that

$$2^{\aleph_\alpha} > \aleph_\alpha$$

for every ordinals α. For all κ, since $\kappa^\kappa = 2^\kappa$ (why?), we have $\kappa^\kappa > \kappa$. $\square$

Theorem 10.13 (Konig)
For all finite κ, we have $\kappa^{\mathrm{cof}(\kappa)} > \kappa$.

Here $\mathrm{cof}(\kappa)$ is cofinality, which we haven't defined yet.

We are going to show that these two theorems are "all we can prove" in ZFC.

There are some trivial things we can prove, like

Lemma 10.14
We have

$$(\kappa^\lambda)^\mu = \kappa^{\lambda\cdot\mu}.$$

Proof. This was like a Math 55 problem. Biject

$$\mathscr{F}(\mu, \mathscr{F}(\lambda, \kappa)) \to \mathscr{F}(\lambda \times \mu, \kappa)$$

in the obvious way. $\square$

§10.6 Some exponentiation is not interesting

Lemma 10.15
Suppose $2 \le \kappa \le \lambda$, and λ is infinite. Then

$$\kappa^\lambda = 2^\lambda.$$

Proof. We have

$$2^\lambda \le \kappa^\lambda \le (2^\kappa)^\lambda = 2^{\kappa\cdot\lambda} = 2^\lambda.$$ $\square$

So we only care about $\kappa > \lambda$ and 2^κ.

§11 October 7, 2014

Last time, we saw that cardinal addition and multiplication were trivial, and that exponentiation is hard to prove stuff about. We only know that

$$\kappa^\lambda = 2^\lambda \quad \forall 2 \le \kappa \le \lambda, \lambda > \omega.$$

It appears that $(\lambda^+)^\lambda$ can be much bigger than λ. For example, if CH is true then $2^{\aleph_0} = \aleph_1 \ll \aleph_1^{\aleph_0}$.

§11.1 Cofinality

Put in a magazine with ω many bullets...

Definition 11.1. Let α be a limit ordinal. A function $f : \beta \to \alpha$ is called **cofinal** if for every $\overline{\alpha} < \alpha$, there is a $\overline{\beta} < \beta$ such that $f(\overline{\beta}) > \overline{\alpha}$. In other words, $\operatorname{im} f$ gets arbitrarily high.

The **cofinality** of α, denoted $\operatorname{cof}(\alpha)$, is the least ordinal β such that $\exists f : \beta \to \alpha$ which is cofinal in α.

Loosely, the cofinality is the smallest ordinal β which can be "stretched out" to get α. Observe that in particular, $\operatorname{cof}(\alpha) \le \alpha$.

Example 11.2

$\operatorname{cof}(\aleph_\omega) = \omega$, because we can stretch $\omega = \{0, 1, \dots\}$ as $\aleph_0, \aleph_1, \dots$ which grows arbitrarily large up to $\aleph_\omega$.

Example 11.3

We have $\operatorname{cof}(\aleph_1) = \aleph_1 = \omega_1$. In general, any successor cardinal has cofinality equal to itself.

Definition 11.4. We say that a limit ordinal α is **regular** if $\operatorname{cof}(\alpha) = \alpha$ and **singular** if $\operatorname{cof}(\alpha) < \alpha$.

The case of interest is when α is a cardinal.

Example 11.5

$\aleph_0 = \omega$, $\aleph_n$ and $\aleph_{\alpha+1}$ are all regular. However, $\aleph_\omega$ is singular, as is $\aleph_{\omega+\omega}$ and so on.

Remark 11.6. There may exist large cardinals $\aleph_\lambda$, with λ a limit ordinal, such that $\aleph_\lambda$ is regular. The question of whether they exist is independent of ZFC. In fact, it turns out their existence establishes the consistency of ZFC; very roughly, they are so big that cutting the universe off at them gives a model of ZFC.

§11.2 Lemmas on cofinality

Lemma 11.7

Suppose α is a limit ordinal, and let $\beta = \operatorname{cof}(\alpha)$. Then there exists a map from β to α which is cofinal and moreover is strictly increasing.

Clearly we have a function $\beta \to \alpha$ cofinal, so the lemma just lets us assume WLOG it is increasing.

Proof. Take the cofinal function $g : \beta \to \alpha$; we wish to modify it so that it's increasing. Define by transifnite recursion the map $f : \beta \to \alpha$ with

$$\gamma \mapsto \max\left(g(\gamma), 1 + \sup_{\overline{\gamma} < \gamma} f(\gamma)\right).$$

This forces f to be strictly increasing and obviously it remains cofinal. Note that we are OK at the top since α is a limit ordinal. □

Lemma 11.8

Let α, β be limit ordinals. Suppose $f : \alpha \to \beta$ is cofinal and non-decreasing. Then $\operatorname{cof}(\alpha) = \operatorname{cof}(\beta)$.

This is pretty clear if you look at a picture.

Proof. First, we prove $\operatorname{cof}(\beta) \le \operatorname{cof}(\alpha)$. Let $g : \operatorname{cof}(\alpha) \to \alpha$ be cofinal.

$$\operatorname{cof}(\alpha) \xrightarrow{g} \alpha \xrightarrow{f} \beta$$

You can check that $f \circ g$ is cofinal, so $\operatorname{cof}(\beta) \le \operatorname{cof}(\alpha)$ by definition (since $\operatorname{cof}(\beta)$ is the minimal one).

Now let's prove $\operatorname{cof}(\alpha) \le \operatorname{cof}(\beta)$. This time let $g : \operatorname{cof}(\beta) \to \beta$ be cofinal, and assume WLOG that it's strictly increasing. We want to construct a cofinal map $h : \operatorname{cof}(\beta) \to \alpha$. Let's have h map $\overline{\beta}$ to the least $\overline{\alpha}$ such that $f(\overline{\alpha}) > g(\overline{\beta})$; this is OK since f is cofinal. one can check that this works. □

§11.3 Given AC, cofinalities and successor cardinals are regular

This gives the following corollary, which we'll call a lemma for kicks.

Lemma 11.9

For any limit ordinal α we have $\operatorname{cof}(\alpha)$ is a regular cardinal.

Proof. First, we prove that $\operatorname{cof}(\alpha)$ is actually a limit ordinal. If not, suppose $\operatorname{cof}(\alpha) = \gamma + 1$. Then we can map γ cofinally into α by shifting everything up by one, contradiction.

Now, we have a cofinal increasing map

$$\operatorname{cof}(\alpha) \to \alpha.$$

By applying the lemma, we have $\operatorname{cof}(\operatorname{cof}(\alpha)) = \operatorname{cof}(\alpha)$. This implies (by definition) that $\operatorname{cof}(\alpha)$ is regular.

Finally, we want to show $\operatorname{cof}(\alpha)$ is a cardinal. If not, there's a bijection between $\operatorname{cof}(\alpha)$ and a smaller ordinal γ, say g. Then $f \circ g$ is a cofinal map into α which is a contradiction. □

Proposition 11.10

Given the Axiom of Choice (or just Countable Choice), $\operatorname{cof}(\aleph_1)$ is regular.

Proof. If not, then $\operatorname{cof}(\aleph_1)$ is a cardinal less than $\aleph_1$; this can only mean $\operatorname{cof}(\aleph_1) = \aleph_0$.

Let $f : \aleph_0 \to \aleph_1$ be cofinal. We observe that $f(n) < \aleph_1$, which means that $f(n)$ is countable. For each n, we can pick a g_n from $\aleph_0$ onto $f(n)$. By "union"-ing all the g_n, we get a surjection from $\aleph_0$ onto $\aleph_1$. Contradiction. $\square$

More generally, we have the following.

Lemma 11.11

Assume Choice. Given that $|A| = \kappa^+$, there is no collection of sets

$$\{A_\alpha \mid \alpha < \kappa\}$$

such that

(1) $\forall \alpha < \kappa$ we have $|A_\alpha| \le \kappa$.

(2) $A = \bigcup_{\alpha<\kappa} A_\alpha$.

Proof. Basically the same. I'll copy it down, but it's not especially worth reading.

Assume not. Each A_α (for $\alpha < \kappa$) has size $\le \kappa$. So there exists surjections for each $\alpha < \kappa$ with codomain

$$\exists f_\alpha : \kappa \to A_\alpha.$$

By AC we can pick such an f_α for each α.

We will now produce a surjection from κ onto $\bigcup_{\alpha<\kappa} A_\alpha$. This will imply $\left|\bigcup_{\alpha<\kappa} A_\alpha\right| \le \kappa$. Let $\pi : \kappa \to \kappa \times \kappa$ be a bijection, and set

$$g : \kappa \times \kappa \to \bigcup_{\alpha<\kappa} A_\alpha$$

by

$$(\alpha, \beta) \mapsto f_\alpha(\beta).$$

Clearly g is surjective, since the f_α are all surjective. Thus

$$g \circ \pi : \kappa \to \bigcup_{\alpha<\kappa} A_\alpha$$

is surjective, completing the proof. $\square$

This gives us the following theorem.

Theorem 11.12

Assume Choice. Then κ^+ is a regular cardinal for every κ.

Proof. It suffices to show that $\operatorname{cof}(\kappa^+) = \kappa^+$, so assume for contradiction that $\operatorname{cof}(\kappa^+) < \kappa^+$. Consider the corresponding map f. Set $A_\alpha = f(\alpha)$; now $\{A_\alpha\}_{\alpha\le\kappa}$ is a partition described in the above lemma, contradiction. $\square$

Theorem 11.13 (Konig)
For every infinite cardinal $\kappa^{\operatorname{cof}(\kappa)} > \kappa$.

Proof. This is just a diagonal construction.
Suppose $f : \operatorname{cof}(k) \to \kappa$ is cofinal. Suppose also for contradiction that

$$\kappa^{\operatorname{cof}(\kappa)} = \kappa.$$

That means we can enumerate all functions $\operatorname{cof}(\kappa) \to \kappa$ as $(g_\alpha)_{\alpha \le \kappa}$.
But let

$$g : \operatorname{cof}(\alpha) \to \kappa$$

by sending β to be the least element in

$$\kappa - \{g_\alpha(\beta) \mid \alpha < f(\beta)\}.$$

What we've done is that for every $\beta \in \operatorname{cof}(\kappa)$, our selection of $g(\beta)$ doesn't match g_α for any $\alpha < f(\beta)$. Since f is cofinal, $f(\beta)$ gets arbitrarily large, and so g does not agree for any g_α. Then $g \notin \{g_\alpha\}_\alpha$, contradiction. $\square$

§11.4 Inaccessible cardinals

Consider the monstrous cardinal

$$\kappa = \aleph_{\aleph_{\aleph_{\ddots}}}.$$

This might look frighteningly huge, as $\kappa = \aleph_\kappa$, but its cofinality is ω as it is the limit of the sequence

$$\aleph_0, \aleph_{\aleph_0}, \aleph_{\aleph_{\aleph_0}}, \dots$$

Definition 11.14. We say κ is **weakly inaccessible** if

(i) $\kappa > \omega$, and

(ii) κ is a regular limit cardinal.

You can show that $\aleph_\kappa = \kappa$ in this case.

Definition. We say κ is a **strong limit** if for all $\lambda < \kappa$, we have $2^\lambda < \kappa$. If κ is strong limit and weakly inaccessible, we say it is **strongly inaccessible**.

Aside: You can check that if κ is strongly inaccessible, then V_κ is a model for ZFC. (The limit implies its closed under Power Set, and inaccessibility gives Replacement). That implies that proving the existence of strongly inaccessible cardinals.

§12 October 9, 2014

We discuss trees and Suslin's Hypothesis (SH).

§12.1 Linear Orders

Definition 12.1. A **linear order** is a pair $(L, \le_L)$ which is reflexive, symmetric, transitive, and linear (meaning any two x and y are comparable). It is **dense** if $\forall x <_L y \in L$ we can find z such that

$$x <_L < z <_L y$$

(here $<_L$ means $\le_L$ but not equal). Finally, we say it is **without endpoints** if $\forall x \in L$, there is a $y_1 <_L x$, and $y_2 >_L x$.

We had the following theorem from Cantor, which shows that in the countable case, any guy which has all the above properties is actually isomorphic to $\mathbb{Q}$.

Theorem 12.2 (Cantor)
Suppose $(A, \le_A)$ and $(B, \le_B)$ are countable dense linear orders without endpoints. Then

$$(A, \le_A) \cong (B, \le_B).$$

Proof. We need a bijection f from A to B which is order-preserving. We'll construct f using what is called a "back and forth argument".

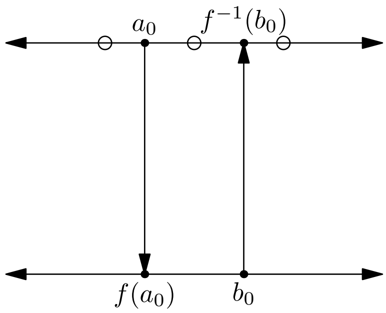
Let $A = \{a_n : n \in \mathbb{N}\}$ and $B = \{b_n : n \in \mathbb{N}\}$. First set $f(a_0)$ arbitrarily. Now we define $f^{-1}(b_0)$ as follows:

- If $b = f(a_0)$ then we're done, $f^{-1}(b_0) = a_0$.
- Otherwise, since $\le_A$ is without endpoints we can let $f^{-1}(b_0)$ be such that

  $$a_0 \le_A f^{-1}(b_0)$$

  iff $f(a_0) \le_B b_0$.

And just rinse and repeat with a_1. If it's already selected, ignore it. Otherwise, since both sides are without endpoints and dense, regardless of which "interval" we can map it preserving order.



We keep going. This exhausts both A and B, because on the even steps we use up the elements in B, and on the odd steps we use up all the elements in A. This gives a bijection f. ∎

Remark 12.3. The theory of dense linear orders is actually complete.

§12.2 Intermission

Question 12.4. Can you generalize the proof to arbitrary cardinalities?

First, let us construct a dense linear order without endpoints of cardinality $\aleph_1$. Consider the set

$$A = \mathbb{Q} \times \omega_1$$

sorted lexicographically. This clearly works. This has a structure of ω_1 embedded in it. So we have like a chain

$$A = \mathbb{Q}_0, \mathbb{Q}_1, \dots, \mathbb{Q}_\alpha, \dots$$

On the other hand we can just run this the other way.

$$B = \dots, \mathbb{Q}_\alpha, \dots, \mathbb{Q}_1, \mathbb{Q}_0.$$

Consider $(\frac{1}{2014}, 0)$. In A, it has countably many things to its left. But every guy in B has uncountably many things to its right. Hence no bijection exists.

We can also do $\mathbb{Q} \times (\omega_1 + 1)$, which is not isomorphic to A. You have a "maximal" $\mathbb{Q}$-blob $\mathbb{Q}_{\omega_1}$, and there's intuitively no way to map this into A. (Check this!)

§12.3 Separable complete linear orders

Definition 12.5. A linear order $(L, \le_L)$ is *complete* if whenever $A \subseteq L$ has an upper bound[5], then there is a *least* upper bound, and similarly for sets bounded below.

Definition 12.6. We say $(L, \le_L)$ is separable if there exists a countable $D \subseteq L$ for which $(D, \le_L)$ is dense.

Now we can prove a generalization of something Cantor did.

Theorem 12.7 (Cantor)

Suppose $(A, \le_A)$ and $(B, \le_B)$ are dense linear orders without endpoints, which are both complete and separable. Then $(A, \le_A) \cong (B, \le_B)$.

Here we've replaced "countable" with "complete and separable".

Proof. Take $\overline{A} \subset A$ which is countable and dense,[6] and similarly define $\overline{B}$. Evidently our first theorem implies

$$(\overline{A}, \le_A) \cong (\overline{B}, \le_B)$$

(just check all the conditions). Let f be the bijection from $\overline{A}$ to $\overline{B}$. We want to lift this to $f : A \to B$. This is easy enough: for any $a \notin \overline{A}$

$$f(a) = \sup_{\le_B} \{ f(\overline{a}) \mid \overline{a} \le_A a \}.$$

We can take sup's by completeness.

To prove this is order-preserving, just notice that if $a_1 <_A a_2$ then we get some $\overline{a} \in \overline{A}$ between them, so $f(\overline{a})$ separates them. (In particular f is injective.)

To prove f is surjective, look at any $b \in B$, take the downwards interval, and then use the fact that A is complete. $\square$

In particular, $(\mathbb{R}, \le_\mathbb{R})$ is the unique dense linear order without endpoints which is complete and separable (note that $(\mathbb{Q}, \le_\mathbb{Q})$ witness separability).

[5]Meaning there exists a $z \in L$ such that $a \le_L z$ for all $a \in A$.

[6]Think of these as "glowing special points" that are scattered all throughout A.

§12.4 Suslin property

Definition 12.8. A linear order $(L, \leq_L)$ has the **Suslin property** if any collection of disjoint open intervals is countable. Here an **open interval** is one of the form

$$(a, b) \stackrel{\text{def}}{=} \{z \in L \mid a <_L z <_L b\}.$$

It might seem that you should be able to pick ω_1 into $\mathbb{R}$, but in fact $\mathbb{R}$ does have the Suslin property – any open interval contains a rational number, so you can pick at most countably many. (But you can embed ϵ_0 into $\mathbb{R}$!)

Lemma 12.9

If a linear order $(L, \leq)$ is separable then it has the Suslin property.

Proof. Let D be a collection of disjoint open intervals, and let $\overline{L}$ be the dense countable subset. By Separability, each open interval contains a distinct element of $\overline{L}$. □

So we can't embed $(\omega_1, \in)$ into there, but we can get order-preserving maps from $(\omega, \in)$, $(\omega^\omega, \in)$, $(\epsilon_0, \in)$, ... Now is it true that you can embed any $\alpha < \omega_1$ in there?

Not sure. We can try transfinite induction. Embedding in $(\mathbb{R}, \leq_\mathbb{R})$ is the same as $((-\infty, 0), \leq_\mathbb{R})$, giving us space on the right to work with. For the transfinite induction the successor case is clear, but for limit ordinals λ we must somehow use the fact that λ is countable (since the induction fails at $\lambda = \omega_1$).

Suppose λ is a limit less than ω_1.[7] So for each α we have an $f_\alpha : \alpha \to \mathbb{R}$ and a bijection $\pi : \lambda \to \mathbb{N}$.

Question 12.10 (Suslin's Hypothesis)**.** Is $(\mathbb{R}, \leq_\mathbb{R})$ the unique dense linear order without endpoints which is both complete and has the Suslin property?

Notice that SP is weaker than separable, and if we replace SP with separable then the answer is "yes".

Definition 12.11. We call a **Suslin line** any other ordering with this property; that is, a dense linear order which is complete, has the Suslin property, but is not separable.

SH is the conjecture that no Suslin lines exist. This would be weird. We can only lie down countably many disjoint union intervals, but the reason is *not* because we can pick a "rational" in every set (by "rational" we mean an element of a separable set).

Theorem 12.12

If ZFC is consistent, then

(a) ZFC + SH is consistent

(b) ZFC + ¬ SH is consistent.

This is proved using something called a Suslin tree. We have the following theorems, which we won't prove.

[7] This can terribly be written as $\lambda \in \mathrm{Lim} \cap \omega_1$.

Theorem 12.13

There is a Suslin line if and only if there is a Suslin tree.

Theorem 12.14

Let L be the constructible universe ("up next"). Then if $V = L$, we have a Susline tree $\neg$ SH.

But we can use a trick called "forcing" as follows: we can put a branch through it to kill it, but then more trees come up, and then it's just massive deforestation. That's how we get another direction.

§13 October 14, 2014

Sick day. What happened?

§13.1 Sparse Review

Given a model (M, E), an assignment to

$$\text{VAR} = \{(7, i) \mid i \in \omega\}$$

is a function $s : \text{VAR} \to M$. We think of $s(\text{“}x_0''\text{)} = s((7, 0)) = a \in M$. Basically, we assign every variable to something in M.

Given a formula φ, $\varphi(x_0, \dots, x_n)$ where the free variables are $x_0, \dots, x_n$ and an assignment $s : \text{VAR} \to M$, the only part that matters for is $s(\text{“}x_0''\text{)}, \dots$

We're going to be lazy and write things like $x \in y$, even though x and y are not actually official variables.

Often we write

$$(M, E) \vDash \phi[\vec{a}]$$

where $\vec{a}$ is really just the part of $s : \text{VAR} \to M$ that is relevant, namely

$$\vec{a} = (s(x_0), \dots, s(x_n)) .$$

(Remember $\vDash$ means “satisfies”.)

Definitions of Δ_0, Σ_n, Π_n.

Δ_0 corresponds to having no unbounded $\forall$ and $\exists$. It means you don't have to look around things.

§14 October 16, 2014

Guest lecture! Today we discuss infinite combinatorics. Unfortunately in my illness I arrived late and failed to get the guest's name.

In finite combinatorics we studied partitions of numbers and rooted trees. Today we will be discussion the generalizations of these to the transfinite.

§14.1 Partitions

We can think of a partition of S as writing

$$S = S_0 \sqcup S_1 \sqcup \cdots \sqcup S_{m-1}$$

as just a function $f : S \to \{0, \dots, m-1\}$ (that is, $f : S \to m$) specifying here to send each element of S.

Definition 14.1. For a set A, let $[A]^n$ be the subsets of size n; i.e.

$$[A]^n = \{x \subseteq A \mid |A| = n\}.$$

Definition 14.2. Let δ be an infinite cardinal. We define a function $f : S \to \delta$ to be a **δ-partition** of S. Given a δ-partition of the $[A]^n$, a set $H \subseteq A$ is called **homogeneous** for f if f is constant on $[H]^n$.

Remark 14.3. It's helpful to think of f as a coloring function on the n-subsets. Homogeneous corresponds to monochromatic.

§14.2 Infinite Ramsey Theorem

Example 14.4

It's well-known from Ramsey theory that any six people, either three are mutual friends or three are mutual stranger. We can rephrase this as saying: any 2-partition of $[6]^2$ has a homogeneous subset of size 3. (Here $[6]^2$ are the edges, and we put them into two colors.)

This is a consequence of the finite Ramsey theorem, but we'll prove an infinite version.

Theorem 14.5 (Infinite Ramsey Theorem)

If A is an infinite set, and $f : [A]^n \to m$ is an m-partition of the n-subsets of A, then there is some countably infinite $H \le A$ homogeneous.

Here (and for the rest of the lecture), m and n will denote natural numbers.

Remark 14.6. When $n = 2$, this states that any m-coloring of an infinite graph has a monochromatic coloring.

Proof. We are going to repeatedly use Infinite Pigeonhole. If $n = 1$, then we are trying to partition $[A]^1 = A$ into a finite pieces, so some part must be infinite, QED.

Now suppose it holds for n. Consider $f : [A]^{n+1} \to m$. For $a \in A$, we define f_a from $[A - \{a\}]^n \to m$ by

$$f_a(x) = f(x \cup \{a\}).$$

By inductive hypothesis, each f_a has an infinite homogeneous subset. Let $H_0 = A$ and a_0 be arbitrary. For $i < \omega$ we define

$$H_{i+1} \subseteq H_i \text{ infinite and homogeneous for } f_{a_i}$$

and then pick $a_{i+1} \in H_{i+1} - \{a_j \mid j \le i\}$.

Now consider $\{a_i : i < \omega\}$. The point is that $\{a_i : i > k\}$ is homogeneous for f_{a_k}. Let the constant value of f_{a_k} on $\{a_i : i \ge k\}$ be $g(i)$. By infinite pigeonhole there is an infinite subset I on which g is constant, as necessary. Then $\{a_i : i \in I\}$ is the desired set. $\square$

The special case of the proof with $m = 3$ colors (RGB, anyone?) and $n = 2$ is more suitable for an olympiad, but makes the above proof much more illuminating. Consider an infinite graph. Take a vertex v_0. Some color emanates infinitely often from v_0. Throw away everything else. Take a new v_1. Ignoring v_0, some color emanates infinitely from v_1. Throw away the other guys (but keep v_1)! In this way we get a sequence $v_0, v_1, \dots$ of vertices, each with a color it really likes. By Pigeonhole, we can take an infinite subset that all like the same color. Done.

§14.3 Some negative results on partitions

Definition 14.7. If κ and δ are cardinals, and $n \in \mathbb{N}$, and α is an ordinal we write $\kappa \to (\alpha)^n_\delta$ if for every δ-partition of $[k]^n$, there is a homogeneous set $H \subseteq \kappa$ for the partition, and H has size α.

Example 14.8

$6 \to (3)^2_2$ and $\omega \to (\omega)^n_m$.

Note that you can increase κ and decrease α, so the $\to$ is "like" an inequality $\ge$.

Why do we assume $n \in \mathbb{N}$? It turns out if AC is given, then we have the following.

Lemma 14.9

Assume AC. Then $\kappa \not\to (\omega)^\omega_2$ for any infinite cardinal κ.

Remark 14.10. People often drop the subscript 2.

Proof. Take a well-ordering $\prec$ of $[\kappa]^\omega$. We'll split κ into two parts using $f : [\kappa]^\omega \to 2$ by

$$f(A) = \begin{cases} 1 & \text{A is } \prec\text{-minimal among the infinite subsets of } A \\ 0 & \text{otherwise.} \end{cases}$$

Assume for contradiction there's some homogeneous $H \subset \kappa$ of size ω; WLOG it's countable.

If H isn't $\prec$-minimal, then consider an infinite $A \in H$ which is. Then f colors A by 1. But H is also an ω-subset of H, so f colors H by 0, contradiction.

So H must be $\prec$-minimal, and since H is homegeneous, so must every infinite subset of H. Select an infinite subset $A_0 \in H$ such that $H - A_0$ is also infinite. By looking at the elements missed by A_0, we can create a chain

$$A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$$

But now we can obtain a decreasing $\prec$ chain

$$H \supseteq A_0 \succ A_1 \succ A_2 \succ \dots.$$

Indeed, each A_i is infinite but is $\prec$-minimal with respect to all its infinite subsets, including A_{i-1}. Boom! $\square$

Lemma 14.11

Assume AC. For any κ, $2^\kappa \not\to (\kappa^+)^2_2$.

Proof. Let $\langle x_\alpha \mid \alpha < 2^k \rangle$ enumerate the binary sequences of κ; i.e. the functions from κ to 2. For each "edge" α, β consider the coloring where

$$\alpha < \beta \to (f(\{\alpha, \beta\}) \iff x_\alpha <_{\text{lex}} x_\beta.$$

Assume for contradiction there's a homogeneous (think monochromatic) subsequence $\langle x_\alpha : \alpha \in H \rangle$, and WLOG it is increasing.

For each i we define

$$\begin{aligned} \beta_i = \min \big\{ \beta \mid \quad & \beta \ge 1 + \sup_{j<i} \beta_j \text{ and} \\ & \exists \alpha > 1 + \sup_{j<i} \alpha_j, \alpha \in H \\ & \text{and } \beta \text{ has 1 in the } \alpha \text{ digit.} \big\} \\ \alpha_i = \min \big\{ \alpha \in H \mid \quad & \alpha > 1 + \sup_{j<i} \alpha_j \\ & \text{ and } \beta_i \text{ has 1 in the } \alpha \text{ digit} \big\}. \end{aligned}$$

Set the sup's as 0 when $i = 0$.

Basically what this does is that as i grows, more digits get fixed. Supremum exists by regularity of κ^+. So you get screwed by the time you get to x_κ. $\square$

Remark 14.12. This is highly similar to the proof that you can't have an $\aleph_1$ increasing sequence of real numbers.

Corollary 14.13

$2^\kappa \not\to (2^\kappa)^2_2$.

Proof. $2^\kappa \ge \kappa^+$. $\square$

§14.4 Large Cardinals

Definition 14.14. A cardinal κ is called **weakly compact** if $\kappa \to (\kappa)^2_2$.

Corollary 14.15

If κ is weakly compact, κ is inaccessible.

Proof. By above stuff, we clearly have $\kappa > 2^\lambda$ for all $\lambda < \kappa$.

Assume for contradiction that κ is singular. Then $\kappa = \bigcup_{i<\lambda} A_i$ where $\lambda < \kappa$ and $|A_i| < \kappa$. Define $f : [k]^2 \to 2$ by

$$f(\{\alpha, \beta\}) = 1 \iff \exists i < \lambda : \alpha, \beta \in A_i.$$

□

§14.5 Trees

Definition 14.16. A **tree** is a poset $(T, <)$ such that for every $x \in T$, the set

$$\text{pred}_T(x) = \{y \in T \mid y < x\}$$

is well-ordered by $<$. The **height** of any x is $\text{ht}(x) = \text{ot}(\text{pred}_T(x))$ and T_α is the set of x's with height α, meaning

$$T_\alpha = \{x \in T \mid \text{ht}(x) = \alpha\}.$$

The height of the whole tree is the smallest α with $T_\alpha \neq 0$, i.e.

$$\text{ht}(T) = \min\{\alpha : T_\alpha = \varnothing\}.$$

A **branch** through T is a maximal linear subset. A κ-tree is a tree of height κ whose levels each have less than κ.

Example 14.17

The tree $2^{<\omega}$ is an ω-tree. The tree $\omega^{<\omega}$ has size ω, but it is very fat and not an ω-tree.

Definition 14.18. An **Aronszajn tree** (pronounced *EH-rin-shine*) is a κ-tree without a branch of size κ.

Lemma 14.19 (Konig's Lemma)

There is no $\aleph_0$-Aronszajn tree.

Proof. At each level there's finitely many guys. So some branch is infinite. Now go up the tree greedily. □

Lemma 14.20 (Aronszajn)

There is an $\aleph_1$-Aronszajn tree.

§15 October 21, 2014

Constructability, Model Theory, ...

§15.1 Definability

Definition 15.1. Given (M, E) a model in LST, we say that a relation $X \subseteq M^n$ is (M, E)**-definable** by $\varphi(x_1, \dots, x_n)$ if

$$X = \{\vec{a} \in M^n \mid (M, E) \vDash \phi[\vec{a}]\}.$$

We say X is (M, E)**-definable** if such a φ exists.

Definition 15.2. We say X is **definable in** (M, E) **with parameters** if there is a formula $\phi(x_1, \dots, x_n, y_1, \dots, y_m)$ and a parameter sequence $\vec{b} \in M^m$ such that

$$X = \left\{\vec{a} \in M^n \mid (M, E) \vDash \varphi[\vec{a}\vec{b}]\right\}.$$

Remark 15.3. Everything in M is definable in (M, E) with parameters. Take $b \in M$ and consider the formula "$x = b$". This has one free variable and one parameter.

Remark 15.4. We'll say $a \in M$ is definable if $\{a\}$ is definable.

Example 15.5

We can write down the formula defining "is an ordinal". We can expand the machine code for transitive: $\forall y \in x (y \subseteq x)$, or $\forall y \in x(\forall z \in y(z \in x))$. This is Δ_0 because it has no unbounded parameters. Similarly expand "well-ordered by $\in$".

Example 15.6

$\varnothing$ is Δ_0 definable. Write the formula $\forall y \in x(y \neq y)$.

We are mainly interested in $\in$**-models**, where M is transitive and $\in|_{M \times M} = E$. We will often write this as $(M, \in)$.

§15.2 Fragments of the Universe

Let's see what is definable over the structure $(V_\omega, \in)$.

Example 15.7

$\omega = \{0, 1, \dots\}$ is Δ_0 definable without parameters in $(V_\omega, \in)$. Get

$$\{a \in V_\omega \mid (V_\omega, \in) \vDash \varphi[a]\} = \{0, 1, \dots\}.$$

where φ means "is an ordinal".

Example 15.8

$\{a \in V_{\omega_1} \mid (V_{\omega_1}, \in) \vDash \varphi[a]\} = \omega_1$ and $\{a \in V \mid (V, \in) \vDash \varphi[a]\} = \mathrm{On}$.

Lemma 15.9

Suppose $(M, \in)$ and $(N, \in)$ are two transitive $\in$-models. Moreover, suppose $M \subseteq N$. Let $\varphi(x_1, \dots, x_n)$ be a formula in LST. Let $\vec{a} \in M^n$ be a parameter sequence. Then

(a) If $\varphi \in \Delta_0$, then $(M, \in) \vDash \phi[\vec{a}] \iff (N, \in) \vDash \phi[\vec{a}]$.

(b) If $\varphi \in \Sigma_1$, then $(M, \in) \vDash \phi[\vec{a}]$ implies $(N, \in) \vDash \phi[\vec{a}]$, but the converse fails.

(c) If $\varphi \in \Pi_1$, then $(N, \in) \vDash \phi[\vec{a}]$ implies $(M, \in) \vDash \phi[\vec{a}]$, but the converse fails.

These are called Δ_0-absoluteness, upward Σ_1-absoluteness, and downward Π_1-absoluteness. This is actually intuitively clear. In the first case, since $\varphi \in \Delta_0$, then truth depends only on things internal to $\vec{a}$, and M and N have the same information in this case. In the second case, we have some existence qualifiers, but setting these to things in M is fine in N as well. Similarly for the third case.

Proof. We prove (a) by induction on formula complexity. In the base case, we have several cases. The first is ϕ is "$x_1 \in x_2$". Given $(a_1, a_2) = \vec{a} \in M^2$, we have

$$(M, \in) \vDash a_1 \in a_2 \iff (N, \in) \vDash a_1 \in a_2.$$

Well, duh. We also have "$x_1 = x_2$", which is clear.

For the inductive step, we assume the statement holds for $\phi(x_1, \dots, x_n)$ and $\psi(y_1, \dots, y_n)$. We just check $\neg\phi(x_1, \dots, x_n)$ and $\phi(x_1, \dots, x_n) \wedge \psi(y_1, \dots, y_m)$.

Do stuff with the other quantifiers. We need the transitivity condition at the bounded quantifier step. If M thinks there exists x in the parameter a, we need N to also think that. Writing it out

$$(M, \in) \vDash \exists y \in x_1 \phi(y, x_1, , , .x_n)[\vec{a}]$$

means by definition

$$\exists b \in a_1 : b \in M \text{ and } (M, \in) \vDash \phi[b, a_1]. \tag{1}$$

On the other end we have

$$(N, \in) \vDash \exists y \in x_1 \phi(y, x_1, , , .x_n)[\vec{a}]$$

means by definition

$$\exists b \in a_1 : b \in N \text{ and } (N, \in) \vDash \phi[b, a_1]. \tag{2}$$

So we need to show the witness statements (1) and (2) are equivalent. To show (1) implies (2), we only need $M \subseteq N$. For the other direction, though, we do need transitivity; we know $b \in a_1$, $b \in N$, $a_1 \in M$, but we want $b \in M$ and that doesn't follow unless M is transitive!

For (b), (c) do similar things. Invoke (a) for convenience. $\square$

§15.3 Definable sets

Definition 15.10. For $(M, \in)$, with M transitive, and define

$$\mathrm{Def}^M = \{X \subseteq M \mid X \text{ definable on } (M, \in) \text{ with parameters}\}.$$

Remark 15.11. We clearly have $M \subseteq \mathrm{Def}^M \subseteq \mathcal{P}(M)$.

Fact 15.12. If $|M| = n \in \mathbb{N}$, then $\left|\mathrm{Def}^M\right| = 2^n$.

Fact 15.13. If $|M| = \alpha \geq \omega$, then

$$\left|\mathrm{Def}^M\right| = \alpha \times \aleph_0 = \alpha.$$

Exercise 15.14. Suppose $(M, \in)$ is an $\in$-model with M transitive.

(1) $(M, \in) \vDash$ Extensionality, Foundation.

(2) $(M, \in) \vDash \varnothing$Emptyset if and only if $\varnothing \in M$, i.e. $M \neq \varnothing$. (Just note that "$x = \varnothing''$ is Δ_0.)

(3) $M \vDash$ Pairing if and only if $\forall x, y \in M$ we have $\{x, y\} \in M$.

(4) ...

(5) ...

(6) $(M, \in) \vDash$ Infinity when $\omega \in M$.

(7) $(M, \in) \vDash$ Comprehension if and only if for every $C \in \mathrm{Def}^M$ and for all $a \in M$, we have $C \cap a \in M$.

The key is Δ_0 – this lets us move back and forth between $(M, \in)$ and V.

§16 October 23, 2014

Today we cover reflection. In what follows, the LST models are *not* necessarily transitive.

§16.1 Model theory notions

Definition 16.1. Suppose $\mathscr{M} = (M, E)$ and $\mathscr{M}' = (M', E')$ are LST-models. We say $\mathscr{M}$ is a **substructure** of $\mathscr{M}'$, written $\mathscr{M} \subseteq \mathscr{M}'$, if $\mathscr{M} \subseteq \mathscr{M}'$ and $E = E' \cap (M \times M)$.

Definition 16.2. We say $\mathscr{M}$ is an **elementary substructure** of $\mathscr{M}'$, written $\mathscr{M} \prec \mathscr{M}'$, if for all ϕ in LST and $\vec{a} \in M^n$, $\mathscr{M} \vDash \phi[\vec{a}] \iff \mathscr{M}' \vDash \phi[\vec{a}]$.

Theorem 16.3 (Tarski-Vaught Test)
Suppose $\mathscr{M}, \mathscr{M}'$ are LST-models such that $\mathscr{M} \subseteq \mathscr{M}'$. Then $\mathscr{M} \prec \mathscr{M}'$ if and only if the following condition holds: Let ϕ be a sentence in LST and $\vec{b} \in M^n$. If $\exists a \in M'$ such that $\mathscr{M}' \vDash \phi[a, \vec{b}]$ then there exists $a \in M$ such that $\mathscr{M}' \vDash \phi[a, \vec{b}]$.

Proof. First, we show (1) implies (2). Assume $\mathscr{M} \prec \mathscr{M}'$. Fix ϕ in LST and $\vec{b} \in M^n$. Suppose $\exists a \in M'$ such that $M' \vDash \phi[a, \vec{b}]$. Then $M' \vDash \exists a \phi[a, \vec{b}]$. Since $\mathscr{M} \prec \mathscr{M}'$,

$$\mathscr{M} \vDash \exists a \phi[a, \vec{b}].$$

Fix such an $\overline{a} \in \mathscr{M}$. So $\mathscr{M} \vDash \phi[\vec{a}, \vec{b}]$. But $\mathscr{M} \prec \mathscr{M}'$, so

$$\mathscr{M}' \vDash \phi[\overline{a}, \vec{b}]$$

as needed.

The converse is the interesting direction. We'll prove (1) by induction on formula complexity. The base case is Σ_0 formulas. $a = b$ means

$$\mathscr{M} \vDash a = b \iff a = b \iff \mathscr{M}' \vDash a = b.$$

Now $a \in b$ is

$$\mathscr{M} \vDash a \in b \iff (a, b) \in E \iff (a, b) \in E' \iff \mathscr{M}' \vDash a \in b.$$

Then for some last things. Negation $\neg$ and or $\vee$ is immediate. We also need bounded quantifiers. Assume it's true for ϕ, so

$$\mathscr{M} \vDash \phi[\vec{b}] \iff \mathscr{M}' \vDash \phi[\vec{b}]$$

Show that for $a \in M$,

$$\mathscr{M} \vDash \exists x \in a \phi(x, \vec{b}) \iff \exists \overline{a} \in M, \overline{a} \in a, \mathscr{M} \vDash \phi[\overline{a}, \vec{b}].$$

Hence $\exists \overline{a} \in M$, $\overline{a} \in a$, such that $\mathscr{M}' \phi[\overline{a}, \vec{b}]$.

Then for the inductive step. Suppose that $\mathscr{M}$ and $\mathscr{M}'$ satisfy the same formulas for Π_n formulas (the Σ_n case follows by negation). Want to show Σ_{n+1} Fix $\phi \in \Sigma_{n+1}$, say

$$\phi = \exists x \psi(x, y_1, \dots, y_n)$$

where $\psi \in \Pi_n$. Suppose

$$\mathscr{M} \vDash \exists x \psi[x, \vec{b}].$$

Pick $a \in M$ such that

$$\mathscr{M} \vDash \psi[a, \vec{b}]$$

so since $\mathscr{M} \prec_{\Pi_n} \mathscr{M}'$ we have

$$\mathscr{M}' \vDash \psi[a, \vec{b}].$$

Hence

$$\mathscr{M}' \vDash \exists x \psi[x, \vec{b}].$$

Hence we have prove than

$$\mathscr{M} \vDash \exists x \psi[x, \vec{b}] \implies \mathscr{M}' \vDash \exists x \psi[x, \vec{b}].$$

We need the converse now. So far we haven't used the Tarski-Vaught condition; we invoke it now and then repeat the proof in the opposite direction. Indeed, just take $a \in M'$ such that $M' \vDash [a, \vec{b}]$. Then $\exists a \in M$ such that $\mathscr{M}' \vDash \psi[a, \vec{b}]$. The inductive hypothesis then finishes the proof. □

Intuitively, what this is saying that $\mathscr{M} \prec \mathscr{M}'$ if for some formula ϕ, if we have a witness a in $\mathscr{M}'$ then we can also get a witness in $\mathscr{M}$.

§16.2 Reflection

Now for the cool stuff.

Definition 16.4. Suppose κ is a regular uncountable cardinal. Then $C \subseteq \kappa$ is a **club** (short for "closed unbounded") if the following holds for all $\alpha < \kappa$

- There exists $\beta \in C$ with $\beta > \alpha$.
- If $\alpha = \sup(C \cap \alpha)$, then $\alpha \in C$.

Theorem 16.5 (Reflection)

Let κ be a regular uncountable cardinal. Let $\langle M_\alpha : \alpha < \kappa \rangle$ be such that

(1) Each $\mathscr{M}_\alpha = (M_\alpha, E_\alpha)$ is an LST-model.

(2) $\mathscr{M}_\alpha \subseteq \mathscr{M}_\beta$ for all $\alpha < \beta < \kappa$.

(3) $|M_\alpha| < \kappa$ for any α.

(4) $M_\lambda = \bigcup_{\alpha<\lambda} M_\alpha$ for any limit λ.

We define $\mathscr{M} = (M, E)$, where $M = \bigcup_{\alpha<\kappa} M_\alpha$ and $E = \bigcup_{\alpha<\kappa} E_\alpha$. Then the set

$$C = \{\alpha < \kappa \mid \mathscr{M}_\alpha \prec \mathscr{M}\}$$

is a club in κ.

Remark 16.6. It follows from this that if $\alpha < \beta$ and $\alpha, \beta \in C$, then $\mathscr{M}_\alpha \prec \mathscr{M}_\beta$.

Proof. Let λ be a limit cardinal less than κ. We wish to show that $C \cap \lambda$ is unbounded in κ. We wish to show $\lambda \in C$, i.e. that $\mathscr{M}_\lambda \prec \mathscr{M}$. In other words, for any ϕ in LST and $\vec{b} \in M_\lambda^n$ we want the equivalence

$$M_\lambda \vDash \phi[\vec{b}] \iff \mathscr{M} \vDash \phi[\vec{b}].$$

Well, $\vec{b}$ gets covered by by some M_α since λ is a limit dude. Now we want to check the Tarski-Vaught test. Suppose $a \in M$, $\mathscr{M} \vDash \phi[a, \vec{b}]$. We want to show there is $a \in M_\lambda$, $\mathscr{M} \vDash \phi[a, \vec{b}]$. So we go down to $\mathscr{M}_\alpha$:

$$\mathscr{M} \vDash \exists x \varphi[x, \vec{b}] \implies M_\alpha \vDash \exists x \varphi[x, \vec{b}]$$

and blah blah blah.

So this shows that C is closed. That's not too interesting, because for all we know C might just be empty. But now we're going to show C is unbounded, which is far more interesting. For ϕ in LST, let

$$f_\phi : \kappa \to \kappa$$

by sending α to the least $\beta < \kappa$ such that for all $\vec{b} \in M_\alpha$, if there exists $a \in M$ such that $\mathscr{M} \vDash \phi[a, \vec{b}]$ then $\exists a \in M_\beta$ such that $\mathscr{M} \vDash \phi[a, \vec{b}]$.

We claim this is well-defined. There are only $|M_\alpha|^n$ many possible choices of $\vec{b}$, and in particular there are fewer than κ of these (this is why we assume $|M_\alpha| < \kappa$). Otherwise, we can construct a cofinal map from $|M_\alpha^n|$ into κ by mapping each vector $\vec{b}$ into a β for which the proposition fails. And that's impossible since κ is regular!

In other words, what we've done is fix ϕ and then use Tarski-Vaught on all the $\vec{b} \in M_\alpha^n$. Now let $g : \kappa \to \kappa$ be defined by

$$\alpha \mapsto \sup_{\phi \in \text{LST}} f_\phi(\alpha).$$

Since κ is regular and there are only countably many formulas, $g(\alpha)$ is well-defined.

Check that if α has the property that g maps α into itself (in other words, α is closed under g), then by the Tarski-Vaught test, we have $M_\alpha \prec \mathscr{M}$.

So it suffices to show there are arbitrarily large $\alpha < \kappa$ which are closed under g. Fix α_0. Let $\alpha_1 = g(\alpha_0)$, et cetera and define

$$\alpha = \sup_{n<\omega} \alpha_n.$$

This α is closed under g, and by making α_0 arbitrarily large we can make α as large as we like. $\square$

§16.3 Variations

Theorem 16.7
Suppose ϕ is in LST and $\vec{b} \in V^n$. If $V \vDash \phi[\vec{b}]$, then there exists α such that $V_\alpha \vdash \phi[\vec{b}]$.

Why is this called reflection? Basically it means any statement ϕ one tries to make about V is destined to fail in the sense that some level V_α will also have the statement.

Theorem 16.8
$C = \{\alpha \in \text{On} \mid V_\alpha \prec_{\Sigma_n} V\}$ is a club in On.

§17 October 28, 2014

Laptop sick day. TODO: fill in.

§18 October 30, 2014

Continuation of last time. (Guess whose laptop was dead?)

§18.1 Completing the proof of a theorem

We were proving $L_\kappa \vDash \mathrm{ZF}$

Proof. See notes. TODO: fill in later. Reflection Theorem is useful because the setup is $L_\kappa = \bigcup_{\alpha<\kappa} L_\alpha$.

...

Let $F \in \mathrm{Def}^{L_\kappa}$ and $F : L_\kappa \to L_\kappa$. We want to show for any set a, F applied pointwise to a lives inside κ.

Assume not. Let $\alpha < \kappa$ be such that $a \in L_\alpha$. We can shoot each element of L_α onto $|\alpha| < \kappa$, and then we get a cofinal map from $|\alpha|$ into κ, contradiction. $\square$

§18.2 The statement $L_\kappa \vDash V = L$

We will show L_κ gives $V = L$, AC, and CH.

We need to prove that

$$\forall x \exists \alpha \, (x \in L_\alpha) \, .$$

This might seem since by definition $L_\kappa = \bigcup_{\alpha<\kappa} L_\alpha$. But this particular statement is in V. We need to prove it in L_κ; i.e. while it's obvious that $V \vDash V = L$, we don't have $L_\kappa \vDash V = L$.

Let $x = L_\alpha$. We want to decide whether $L_\kappa \vDash (x = L_\alpha)$. In other words, we defined L_α in V, and we want to check we get the same thing as if we run the definition in L (or L_κ).

Like assuming ZFC is consistent, we can construct a model M^* of ZFC which is not well-founded by adding on the condition $\alpha_1 > \alpha_2$, $\alpha_2 > \alpha_3$, ... This is consistent by compactness (look it up): for the model to be inconsistent, it must have a finite set of inconsistent statements. And if we run the definition of L in here, we get something else

In still other words, what we really want to do is show that if we run the definition of L_κ inside itself, we get all of L_κ. So our goal it look at the definition of $\langle L_\alpha : \alpha < \kappa \rangle$ and check that it is simple enough that we have absoluteness. Since L_κ is transitive, we'd be done if this was Δ_0 – but it's not. In fact, we will show it is Σ_1. This is sufficient because we then have

$$L_\kappa \vDash (x \in L_\alpha) \implies V \vDash (x \in L_\alpha) \, .$$

For this we use something like Godël encoding. First we need to get the language, which we've already done. Then we have to define what a term is. Then we need to define a formula sequence; it's just going to be a finite sequence where you build up the formula. Next you define the length of a formula. It turns out that all these things so far are Δ_0. Finally you define satisfaction sequence and definability in Σ_1.

In the end by encoding syntax (with some fairly scary computations) that

- "x is the αth level of the L-hierarchy", that is, L_α, is Σ_1-definable.
- "x is constructible" is Σ_1 since it is $\exists y, \alpha \, (\mathrm{Lev}(y, \alpha) \wedge x \in y)$.
- $V = L$ is the statement $\forall x \, (y \text{ is constructible})$, so it is Π_2.

Exercise 18.1. Assume $\lambda > \omega$ is a limit ordinal. Show that for all α such that $\omega < \alpha < \lambda$, we have

$$L_\lambda \vDash \mathrm{DEF}(L_{\alpha+1}, L_\alpha).$$

Here the $L_{\alpha+1}$ and L_α are the real thing.

Proof. Check that $\mathrm{DEF}(x, y)$ is Σ_1. Check that $L_{\alpha+1}$ is a Σ_1 formula. □

The converse of what we want is also a thing.

Theorem 18.2
If M is transitive and $M \vDash V = L$ then $M = L_\lambda$ for some limit ordinal λ.

Proof. Since $M \vDash V = L$, and α first appears in $L_{\alpha+1}$, the sup of the ordinals in M must be a limit ordinal, say λ.

Consider $x \in M$. Since $M \vDash V = L$, there exists b, α such that $M \vDash \mathrm{LEV}(b, \alpha) \wedge x \in b$. But (and this is the point), the statement $\mathrm{LEV}(b, \alpha)$ is Σ_1. So by Σ_1-upward absoluteness, we get $V \vDash \mathrm{LEV}(b, \alpha)$. Hence $b = L_\alpha$.

Thus $x \in b = L_\alpha$. Hence we showed that for all $x \in M$, $x \in L_\alpha$ for some $\alpha < \lambda$. Consequently $M \subseteq L_\lambda$. Thus $M = L_\lambda$. □

Now here's what we want.

Theorem 18.3
If λ is a limit ordinal, then $L_\lambda \vDash V = L$.

Proof. Fix $x \in L_\lambda$. Let $\alpha < \lambda$ be such that $x \in L_\alpha$. It suffices to show that $L_\lambda \vDash \mathrm{LEV}(L_\alpha, \alpha)$.

We expand the definition of LEV. Use the fact that L_λ has the function sequence witnessing this Σ_1 fact.

Like basically, it turns out there's a φ, f such that

$$V \vDash \exists f \left(\varphi[f, L_\alpha, \alpha)\right.$$

and you can show $f \in L_\lambda$. □

The key point is the following lemma.

Lemma 18.4
If λ is a limit ordinal then for all $\alpha < \lambda$,

$$\langle L_\beta \mid \beta < \alpha \rangle \in L_\lambda.$$

In fact,

$$\langle L_\beta \mid \beta < \lambda \rangle = \mathrm{Def}^{L_\lambda}.$$

Corollary 18.5
In ZFC^+, $L_\kappa \vDash V = L$. So we have $L_\kappa \vDash \mathrm{ZF} + (V = L)$.

Remark 18.6. We only need the κ condition to guarantee that $V = L$ holds, but we need regularity to cause it satisfy ZF. As an example, both models L_ω, $L_{\omega+\omega}$ implies $V = L$ but not ZF.

§18.3 A Nice application of Reflection

Proposition 18.7
Assuming ZFC$^+$, there exists a countable α for which L_α satisfies ZF.

Proof. By Reflection, the set $D = \{\alpha < \kappa \mid L_\alpha \prec L_\kappa\}$ is a club in κ. Hence for each $\alpha \in D$, we have $L_\alpha \vDash \text{ZF}$.

Using Choice ($L_\kappa \vDash \text{AC}$), we can get a model $M \prec L_\kappa$ such that $M \in L_\kappa$ and $|M| = \aleph_0$. (This is the same argument as last time right before we did the Mostowski collapse.) Now exactly like last time we can let $\overline{M}$ be the transitive collapse of M; hence $\overline{M}$ is transitive and $\overline{M}$ satisfies ZF and $V = L$. The only transitive sets with $V = L$ are L_α by the earlier theorem, and since M is countable, we have $\alpha < \omega_1$. $\square$

§18.4 A sketch of the proof that $L_\kappa \vDash$ AC

Induction. Assume we have a well-ordering of L_α. We wish to get an ordering of $L_{\alpha+1}$. But

$$L_{\alpha+1} = \text{Def}^{L_\alpha} = \left\{ x \in L_\alpha \mid L_\alpha \vDash \varphi[x, \vec{b}] \right\}.$$

Here ϕ is in LST and $\vec{b}$ is a vector of L_α We can well order the countably many formulas of φ_i, we can order $\vec{b}$ lexicographically, and then lexicographically order the entire set.

The limit ordinals are just unions.

In fact we get more that Choice in L_κ – we can order the entire universe. More on that next time.

§19 November 4, 2014

Today we will finish constructibility. The goal is to show that L_κ implies AC, GCH, and a principle $\diamond$ to be defined later.

§19.1 Axiom of Choice

Theorem 19.1

Hence we have shown that $\mathrm{ZF} + (V = L) \implies AC$. Hence $L_\kappa \vDash \mathrm{AC}$.

You need κ to be inaccessible to get $\kappa \vDash \mathrm{ZF}$. But you only need κ a limit to get $V = L$.

Proof. We want a function F from the $\omega, \omega+1, \dots$ to V sending α to a $<_\alpha$ such that for $\alpha \ge \omega$, the following conditions hold:

(1) $<_\alpha$ is a well-ordering of L_α.

(2) $\alpha < \beta \implies <_\alpha \subseteq <_\beta$. Moreover, for any $x \in L_\alpha$ and $y \in L_\beta - L_\alpha$, we have $x <_\beta y$.

(3) There exists a Σ_1 formula $\phi(x_0, x_1, x_2)$ such that for every limit ordinal $\lambda \ge \omega$, we have

$$(L_\lambda \vDash \phi[a, x, V_\omega]) \iff (\alpha \in \mathrm{On} \vee x = <_\alpha).$$

Here's a sketch of how to do this. We can define $<_\omega$ because V_ω consists of a bunch of finite layers. Let $\langle \varphi_i : i < \omega \rangle$ be a Σ_1-definable well-ordering of all the formulas in LST (possible since they live in V_ω). So you can just lex order everything!

To be explicit – suppose we have $<_\alpha$ defined and want to define $<_{\alpha+1}$. We have by definition

$$L_{\alpha+1} = \left\{ x \subseteq L_\alpha \mid x \in \mathrm{Def}^{L_\alpha} \right\}$$

So every element of $L_{\alpha+1}$ is of the form

$$x = \{ z \in L_\alpha \mid \varphi_i[z, a_1, \dots, a_n] \}$$

so we can associate with each x a tuple $(i, a_1, \dots, a_n)$ and then just lex-order it. (Since you can possibly get multiple tuples, you should take the smallest one.)

For λ a limit ordinal, we write $<_\lambda = \bigcup_{\alpha<\lambda} <_\alpha$. ☐

§19.2 GCH

Lemma 19.2 (Condensation)

Assume $\mathrm{ZF} + (V = L)$. Suppose $X \prec L_\lambda$ is an elementary substructure which is transitive. Then

$$(X, \in) \cong L_{\overline{\lambda}}$$

for some limit ordinal $\overline{\lambda}$.

Remark 19.3. It follows that if X is an elementary substructure of L_ω (not necessarily transitive) then $X \cong L_\omega$.

Proof. Since $\in$ is well-founded and extensional, we can take the Mostowski collapse of $(X, \in)$ to get $\pi : (X, \in) \to (\overline{X}, \in)$, where $\overline{X}$ is transitive. We know $L_\lambda \vDash (V = L)$, so $X \vDash (V = L)$ (by the assumption $X \prec L_\lambda$), thus $\overline{X} \vDash (V = L)$. But we already proved that the transitive sets which satisfy $V = L$ are precisely $L_{\overline{\lambda}}$.

It remains to show that $\overline{\lambda}$ is a limit. But this follows from the fact that L_λ thinks "$\forall \alpha$, $\alpha + 1$ exists", and this propagates down to $L_{\overline{\lambda}}$, QED. $\square$

Theorem 19.4

ZF + $(V = L) \implies$ GCH, and hence $L_\kappa \vDash$ GCH. Here GCH is the statement $\kappa^+ = 2^\kappa$ for any infinite cardinal κ.

Proof. Note that ZF + $(V = L)$ implies AC, so we use Choice freely here.

By Cantor, $2^\kappa \ge \kappa^+$, so it suffices to prove that $2^\kappa \le \kappa^+$. But we also showed in homework that

$$|L_{\kappa^+}| = \kappa^+.$$

(Actually, we proved $|L_\alpha| = |\alpha|$ for any α.) Hence, it suffices to show that any subset $A \subseteq \kappa$ in L is actually in L_{κ^+}, because then we've squeezed 2^κ into a space of cardinality κ^+. In other words, we will show $\mathcal{P}(A) \subseteq L_{\kappa^+}$ where the power set is taken over L.

Consider any $A \subseteq \kappa$. Let $\lambda > \kappa$ be a limit. As in the proof of Reflection, we can take $X \prec L_\lambda$ such that $|X| = \kappa$, $A \in X$, and $\kappa \subseteq X$. Let $\pi : (X, \in) \to (L_{\overline{\lambda}}, \in)$ be the transitive collapse in Condensation. We claim that $A \in L_{\overline{\lambda}}$. Indeed,

$$\pi(A) = \{\pi(\gamma) \mid \gamma \in A\}.$$

But π acts as the identity on κ (check this by transfinite induction), and it follows that $\pi(A) = A$.

However,

$$\left|L_{\overline{\lambda}}\right| = |X| = \kappa < \kappa^+.$$

Thus $A = \pi(A) \in L_{\overline{\lambda}}$. $\square$

§19.3 Hulls

Let me write down the details for "as in the proof of reflection", since I've messed this up twice. Here's what we do. By Tarski-Vaight it suffices to find an X such that for all φ in LST and for all $\vec{b} \in X$, if we have witnesses $a \in L_\lambda$ establishing $L_\lambda \vDash \varphi[a, \vec{b}]$, then we can find a witness $a \in X$ establishing

$$L_\lambda \vDash \varphi[a, \vec{b}].$$

Now we define X by recursion as follows. Set

$$X_0 = \kappa \cup \{A\}.$$

This is our "initial set" of things we want X to have at the end of the day. Then we let

$$X_1 = \bigcup_{\substack{\phi \in \text{LST}, \vec{b} \in X_0^\omega \\ L_\lambda \vDash \exists z \phi[z, \vec{b}]}} \left\{ a \in L_\lambda \mid a \text{ is } <_\lambda\text{-minimal and} L_\lambda \vDash [a, \vec{b}] \right\}.$$

OK, that's retarded because the union is over a bunch of singleton sets. But I think that makes the point. Basically, we've thrown in parameters in L_λ such that X_1 satisfies

Tarski-Vaught for all ϕ when the parameters are in X_0. The problem is now we have some elements in $X_1 \setminus X_0$ which can also be parameters. So we construct X_{n+1} based on X_n in the same way.

Hence X_{n+1} works for parameters in X_n, and moreover $X_n \subseteq X_{n+1}$. By taking $X = \bigcup_{n<\omega} X_n$, now X satisfies the Tarski-Vaught test.

Now we claim $|X| = |X_0| = \kappa \geq \omega$. This just follows that any step, we only added in $\omega \cdot \kappa^\omega = \kappa$ many things.

Apparently these things are called hulls.

Theorem 19.5

Assume ZFC$^+$, so κ is a strongly inaccesible cardinal. There is a countable transitive model of ZFC.

Proof. As in the proof of reflection, one can exhibit $X \prec V_\kappa$ countable. Then take the Mostowski collapse of X.

Details: let $X_0 = \{\varnothing\}$. We construct a sequence of countable sets X_n inductively as follows. Consider a sentence $\phi \in \text{LST}$ and for a parameter sequence $\bar{b} \in X_n$ such that $V_\kappa \vDash \exists z \phi[z, \bar{b}]$. Then we take the any such z, and add it into X_n. We let X_{n+1} be the result.

Since X_n was countable, the set $\phi \times X_n^{<\omega}$ of possible pairs of sentences and parameters is countable, and hence we add in at most countably many new elements; hence X_{n+1} is countable.

Then $X = \bigcup X_n$ is countable and is an elementary substructure of V_κ. Now take the Mostowski collapse of X. $\square$

§19.4 Summary

We have shown the following.

- ZF + $(V = L)$ implies AC and GCH.
- $L_\kappa \vDash \text{ZF} + (V = L)$.
- $L_\kappa \vDash \text{ZF} + (CH)$.

So assuming ZFC$^+$, we have demonstrated that ZFC cannot establish $\neg$CH. Later we will use forcing to show that ZFC cannot prove CH either.

But actually we showed more than $L \vDash \text{CH}$. We showed that every real number (subsets of $\mathbb{N}$) appears in L_{ω_1}. So we ask, where do the real numbers appear? For which α do we have get a new real at some level? That's searching for solutions to

$$\mathcal{P}(\omega) \cap L_{\alpha+1} \supsetneq P(\omega) \cap L_\alpha.$$

Fact 19.6. Suppose $\mathcal{P}(\omega) \cap L_{\lambda+1} \neq P(\omega) \cap L_\lambda$. Then there exists a function $f \in L_{\lambda+1}$ such that $f : \omega \to L_\lambda$ which is onto.

In other words, the witness that L_λ is countable appears immediately after a new real number appears.

Next time: β-gap theorem.

§20 November 6, 2014

We'll finish with some more consequences of condensation.

§20.1 β-Gaps

Definition 20.1. For ordinals α, β a **β-gap** is a segment

$$[\alpha, \alpha+\beta] = \{\gamma \text{ ordinal} \mid \alpha \le \gamma \le \alpha+\beta\}$$

such that $P(\omega) \cap L_\gamma$ is empty for each γ in the interval. In other words, $P(\omega) \cap (L_{\alpha+\beta} - L_\alpha)$.

Theorem 20.2

Assume ZF and $V = L$. Then for all $\beta < \omega_1$ there is a β-gap $[\alpha, \alpha+\beta]$ such that $\alpha+\beta < \omega_1$.

Proof. We're interested in gaps less than ω_1 since all the reals appear by L_{ω_1}. Like clearly we can select a gap

$$[\alpha', \alpha'+\beta] \in L_{\omega_2}.$$

Actually, we are going to use the obvious statement to prove the non-obvious statement. Using hulls, we can let $X \prec L_{\omega_2}$ be countable such that $[\alpha', \alpha'+\beta] \subseteq X$. Hence,

$$L_{\omega_2} \vDash \left(P(\omega) \cap (L_{\alpha'+\beta} - L_{\alpha'}) = \varnothing\right).$$

Hence X satisfies this.

Denoting by $\pi : X \to L_\lambda$ be the Mostowski collapse; we have $\lambda < \omega_1$. We set $\alpha = \pi(\alpha')$ an ordinal (since "is an ordinal" is Δ_0). By the definition of π, we see that $\alpha + 1 = \pi(\alpha'+1)$, and so on. Hence the segment is preserved. Now since L_λ is an elementary substructure of L_{ω_1} it follows that $[\alpha, \alpha+\beta]$ is still a gap. To be pedantic,

$$L_\lambda \vDash \left(\mathcal{P}(\pi(\omega)) \cap \left(L_{\pi(\alpha')+\pi(\beta)} \setminus L_{\pi(\alpha')}\right) = \varnothing\right).$$

$\square$

§20.2 A Taste of Fine Structure

Work in ZF + $(V = L)$ and let λ be a limit ordinal. In our proof of GCH, we showed that for any cardinal κ, if $A \subseteq \kappa$ appears in $L_{\lambda+1} \setminus L_\lambda$, then in L there is a function $f : \kappa \to L_\lambda$ which is onto. This implies that $|L_\lambda| = \kappa$; from this CH follows.

Now we actually claim that the collapsing function exists in $L_{\lambda+1}$. In other words, the moment a new subset appears above L_λ, we immediately also see a witness f that collapses all of L_λ onto κ.

Theorem 20.3

Assume ZF and $V = L$. Let κ be a cardinal and A any subset of κ such that $A = L_{\lambda+1} \setminus L_\lambda$ for some limit ordinal λ. Then there exists a function f definable over L_λ which collapses κ onto L_λ.

Proof. We have an order $<_L$ of L_λ which is Σ_1-definable. Let ψ be the formula giving L_λ. By assumption,

$$A = \{x \in L_\lambda \mid L_\lambda \vDash \varphi_A[x, p_A]\}$$

for some formula ϕ_A and parameters p_A in L_λ. It is important right now that we select p_A to be the $<_L$-least parameter which works for the choice of φ_A.

Using hulls, we let X be an elementary substructure of L_λ such that $\kappa \cup \{p_A\} \subseteq X$. (Note that X may be a class here.) Via condensation again we take the Mostowski collapse

$$\pi : X \to L_{\overline{\lambda}}.$$

Claim. $\overline{\lambda} = \lambda$! That means the collapse did not actually collapse anything.

Proof. We wish to show A is in $L_{\overline{\lambda}+1} - L_{\overline{\lambda}}$; hence it suffices to show A is definable over $L_{\overline{\lambda}}$. Since $\kappa \subseteq X$, π acts as the identity on κ, thus $\pi(A) = A$.

Recalling that A consists of ordinals $\alpha < \kappa$, we have

$$\begin{aligned} \alpha \in A &\iff L_\lambda \vDash \varphi_A[\alpha, p_A] \\ &\iff X \vDash \varphi_A[\alpha, p_A] \\ &\iff L_{\overline{\lambda}} \vDash \varphi_A[\pi(\alpha), \pi(p_A)] \\ &\iff L_{\overline{\lambda}} \vDash \varphi_A[\alpha, \pi(p_A)]. \end{aligned}$$

Thus A is definable over $L_{\overline{\lambda+1}}$. ■

Claim. The map π is actually the identity, implying $X = L_\lambda$.

Proof. We use the fact that p_A is $<_L$-minimal. By looking at π, we say that $\pi(p_A)$ is the $<_L$-least set of parameters for which

$$\pi(A) = \left\{\pi(\alpha) \in L_\lambda \mid L_\lambda \vDash \varphi_{\pi(A)}[\varphi(\alpha), \varphi(p_A)\right\}.$$

We showed $\pi(A) = A$ and $\pi(\alpha) = \alpha$. Thus $p_A = \pi(p_A)$. The point is that because we select p_A to be $<_L$-minimal, then when we look at the projected version and notice $\pi(A) = A$ and $\pi(\alpha) = \alpha$, we find that the resulting $\pi(p_A)$ gets exactly the same thing.

But in any case we defined $L_{\overline{\lambda}}$ based solely on the images of $\pi(\alpha)$ for $\alpha < \kappa$ and the image $\pi(p_A)$. Since π is the identity here. Hence $X = L_\lambda$. ■

This gives, in $L_{\lambda+1}$, a function f which maps κ onto L_λ.

CORRECTION: Let $n \in \omega$ such that the formula ϕ_A and ψ (which is Σ_1) are Σ_n. Take a $X \prec_{\Sigma_n} L_\lambda$ substructure, not an arbitrary one. □

§20.3 The Guessing Sequence

This is $\diamond$.

As a reminder, here is the definition of a club.

Definition. Suppose κ is a cardinal which is regular and uncountable. Then $C \subseteq \kappa$ is a **club** if

- C is closed, meaning it contains all its limit points. Precisely, if λ is a limit ordinal less than κ, if $C \cap \lambda$ is unbounded then $\lambda \in C$.
- C itself is unbounded.

Exercise 20.4. The intersection of $(C_\alpha)_{\alpha=0}^{\gamma}$ is a sequence of clubs in κ (where $\gamma < \kappa$) is also a club in κ.

Example 20.5

Let $\kappa = \omega_1$. Examples of clubs in κ are ω_1, (α, ω_1), $\mathrm{Lim} \cap \omega_1$.

Think of clubs in κ as "measure 1 sets". They are pretty fat.

Definition 20.6. A set S is **stationary** if $S \cap C \neq \varnothing$ for a clubs C.

Remark 20.7. Since the intersection of two clubs is a club (which is nonempty), every club is stationary.

Example 20.8

Set $\kappa = \omega_2$. Then

$$S_\omega^{\omega_2} = \{\alpha < \omega_2 \mid \mathrm{cof}(\alpha) = \omega\}$$

Definition 20.9. We define $\diamond$ as the following claim: there exists a sequence $(A_\alpha)_{\alpha<\omega_1}$ such that for any $A \subseteq \omega_1$, the set

$$\{\alpha < \omega_1 \mid A \cap \alpha = A_\alpha\}$$

is stationary, and moreover we have the identity $A_\alpha \subseteq \alpha$. Such a sequence is called a **$\diamond$-sequence** or **guessing sequence**.

Proposition 20.10

$\diamond \implies$ CH.

Proof. Let $x \in \omega$ correspond to a real number. The set of correct guesses A_α is a stationary set; i.e.

$$\{\alpha < \omega_1 \mid x \cap \alpha = A_\alpha\}.$$

Take any α in here such that $\alpha \geq \omega$. Thus

$$A_\alpha = x \cap \alpha = x.$$

Thus every x is an element of the universal $\diamond$-sequence

$$\langle A_\alpha : \alpha < \omega_1 \rangle.$$ $\square$

This is insanely powerful. Basically, every subset A of ω_1 is approximated by a stationary set S_A as described. In other words,

$$A = \bigcup \{A_\alpha \mid \alpha \in S_A\}$$

and the A_α are guess the initial segments.

We won't have time to prove this, but this in fact implies the following.

Theorem 20.11

ZF and $V = L$ implies $\diamond$.

Theorem 20.12

$\diamond$ implies the existence of a Suslin tree; hence Suslin's hypothesis fails.

Hence, assuming ZFC is consistent, ZFC cannot prove SH.

§21 November 11, 2014

Today we start forcing!

We have already shown that

- (Gödel) $\mathrm{ZFC} + (V = L) \implies \mathrm{CH}$.
- (Jensen) $\mathrm{ZFC} + (V = L) \implies \neg\mathrm{SH}$ (through $\diamond$).

and moreover, if ZFC is consistent so is $\mathrm{ZFC} + (V = L)$.

We now move on the following theorems, assuming ZFC is consistent.

- (Cohen) ZFC does not imply CH.
- (Martin and Solowry) ZFC does not imply $\neg$SH.

§21.1 Problems with trying to set up Forcing

Showing Cohen's theorem is very hard; he apparently nearly lost his mind.

To show that ZFC cannot prove $\neg$CH, we used L. These are the obstructions this time.

- We can't use L again for this direction, so we need something new.
- Moreover, L is already the minimal inner model which (1) satisfies ZFC, (2) is transitive, and (3) contains the ordinals. So we can't construct some "inner model" of ZFC.
- It is not possible to prove (in ZFC) that one can extend L to L'. If we somehow knew $V \neq L$ we could do this, but the problem is that $V = L$ is in fact consistent with ZFC.

In light of problem 3, suppose we are in a worst-case scenario in which we are in a model of $\mathrm{ZFC} + (V = L)$. To make things simpler let's assume there is an inaccessible κ, so we have models (such as L_κ) of ZFC.

Let $X \prec L_\kappa$ be such that $|X| = \omega$ and let $\pi : X \to L_\lambda$ be the Mostowski collapse. So, we have $L_\lambda \vDash \mathrm{ZFC} + (V = L)$. But L_λ is countable, so there exists a real number x which is not in L_λ.

Let's define $L_\lambda[x]$ by setting by transfinite recursion

- $L_0[x] = x$
- $L_{\alpha+1}[x] = \mathrm{Def}_x^{L_\alpha[x]}$
- $L_\lambda[x] = \bigcup_{\alpha<\lambda} L_\alpha[x]$.

Finally, we set $L[x] = \bigcup_{\alpha\in\mathrm{On}} L_\alpha[x]$. Clearly if $x \in L$ then $L[x] = L$. But for our choice of λ we have $L_\lambda[x] \neq L_\lambda$.

Now suppose we select $x \in L_{\alpha+1} \setminus L_\alpha$ (here $\alpha > \lambda$), meaning $L_{\alpha+1}[x] = L_{\alpha+1}$ and $L_\gamma[x] \neq L_\gamma$ for every $\gamma \le \alpha$.

We cross our fingers that $L_\lambda[x]$ satisfies $\mathrm{ZFC} + (V \neq L)$ Only then do we even have a hope of refuting CH in this model. Let's prove the easy part now.

Proposition 21.1

As defined above, $L_\lambda[x] \vDash (V \neq L)$.

Proof. The constructible part of L in $L_\lambda[x]$ is the true L_λ, so $L_\lambda[x]$ can see that x is not in L_λ. $\square$

But the real issue is showing that $L_\lambda[x]$ actually satisfies ZFC. In fact, this is in general not even true. To see why, note that $|L_\lambda|$ is countable, so there is some $x \subseteq \omega$ such that there exists a bijection from x to L_λ. For such an x, we claim that

$$L_\lambda[x] \nvDash \mathrm{ZFC}.$$

Assume not. Then we could decode x to get a surjection $f : \omega \to \lambda$ which violates Replacement, as $\lambda \notin L_\lambda[x]$.

§21.2 Coding; good and bad reals

What does coding mean? First, let $f; \omega \to \omega \times \omega \times \omega$ be a canonical bijection. For $n \in \omega$, we write $f(n) = (n_1, n_2, n_3)$. Now we can use the first coordinate to code the domain and the second coordinates to code the $\in$-relation. Consider real $x \subseteq \omega$ such that

$$(D, E) \overset{\text{def}}{=} (\{n_1 \mid n \in \omega\}, \{(n_2, n_3) \mid n \in \omega\})$$

so that E is a well-founded extensional on D. Since $(L_\lambda, \in)$ is countable there exists an $x \subseteq \omega$ such that $(D, E) \cong (L_\lambda, \in)$ via the Mostowski collapse. Then when $L_\lambda[x]$ takes decrypts x and takes the transitive collapse, it gets the entire universe L_λ, which is a terrible violation of Replacement.

Thus, there exist "bad" reals x over L_λ. But good reals can do anything. You might find reals x such that $L_\lambda[x] \vDash \mathrm{ZFC}$, $L_\lambda[x] \vDash \mathrm{ZFC} + \neg\mathrm{CH}$, $L_\lambda[x] \vDash \mathrm{ZFC} + (2^{\aleph_0} = \aleph_{17})$. And in fact, there are!

Our goal is to show that L_λ knows everything about $L_\lambda[x]$ other than x. In other words, we want L_λ can approximate truth in $L_\lambda[x]$.

§21.3 Ground Models

Definition 21.2. More generally, we work with arbitrary transitive models $(M, \in)$ of ZFC, called the **ground model**, with M being countable. We will let M contain a partial order $\mathbb{P} = (P, \leq_P)$ which will exhibit a **generic extension** $M[G]$.

We will show that

(A) (Existence) $M[G]$ exists, in the same way we showed $L_\lambda[x]$ exists. This will be the easy part.

(B) (Truth) Truth in $M[G]$, meaning truth in $M[G]$ can be suitably approximated in M.

(C) (Preservation) $M[G] \vDash \mathrm{ZFC}$, which follows from above.

(D) (Control) By picking $\mathbb{P} \in M$ carefully, we can arrange $M[G] \vDash \mathrm{ZFC} + \text{whatever}$.

§22 November 13, 2014

§22.1 The generic extension $M[G]$

Let M be a transitive model of ZFC (this is stronger than assuming ZFC is consistent). Let $\mathbb{P} = (P, \leq) \in M$ be a partial order with a maximal element $1_{\mathbb{P}}$ which lives inside a model M. The elements of $\mathbb{P}$ are called **conditions**; because they will force things to be true in $M[G]$.

Definition 22.1. A subset $D \subseteq \mathbb{P}$ is **dense** if for all $p \in \mathbb{P}$, there exists a $q \in D$ such that $q \leq p$.

Examples of dense subsets include the entire P as well as any downwards slice.

Definition 22.2. For $p, q \in \mathbb{P}$ we write $p \parallel q$, saying "p is **compatible** with q", if there is exists $r \in \mathbb{P}$ with $r \leq p$ and $r \leq q$. Otherwise, we say p and q are **incompatible** and write $p \perp q$.

Definition 22.3. We say that $A \in \mathcal{P}$ is an **antichain** if for any distinct p and q in A, we have $p \perp q$. An antichain is called a **maximal antichain** if it cannot be extended; i.e. for every $r \in \mathbb{P}$, $r \parallel p$ for some $p \in A$.

Definition 22.4. A set $G \subseteq \mathbb{P}$ is M**-generic** if

(a) If $p \in G$, then for all $q \geq p$, $q \in G$. In other words, we require that G is upwards-closed.

(b) For any $p, q \in G$, there exists a point $r \in G$ such that $r \leq p$ and $r \leq q$ holds *simultaneously*. In other words, any pair of elements in G is compatible.

(c) For all D *in the model* M, if D is dense then $G \cap D \neq \varnothing$.

A set which only satisfies the first two conditions is called a **filter**.

From the last condition we deduce that $G \neq \varnothing$ (since $D = \mathbb{P}$ is dense), and hence it follows $1_{\mathbb{P}} \in G$.

Notice that if $p \geq q$, then the sentence $q \in G$ tells us more information than the sentence $p \in G$. In that sense q is a *stronger* condition. In another sense $1_{\mathbb{P}}$ is the weakest possible condition, because it tells us nothing about G; we always have $1_{\mathbb{P}} \in G$ since G is upwards closed.

Exercise 22.5. Show that in the definition of "M-generic" we can replace "for all dense D" with "for all maximal antichains A".

Sketch of Solution. Show that for every dense set, you can construct an antichain through it. Need AC. □

§22.2 Existence of generic extensions

Theorem 22.6 (Rasiowa-Sikorski Lemma)

Suppose M is a *countable* transitive model of ZFC and $\mathbb{P}$ is a partial order. Then there exists an M-generic filter G.

Proof. Since M is countable, there are only countably many dense sets (they live in M!), say

$$D_1, D_2, \dots, D_n, \dots \in M.$$

Using AC, let $p_1 \in D_1$, and then let $p_2 \le p_1$ such that $p_2 \in D_2$ (this is possible since D_2 is dense). In this way we can inductively exhibit a chain

$$p_1 \ge p_2 \ge p_3 \ge \dots$$

with $p_i \in D_i$ for every i.

Hence, we want to generate a filter from the (p_i). Just take the upwards closure – let G be the set of $q \in \mathbb{P}$ such that $q \ge p_n$ for some n. By construction, G is a filter (this is actually trivial). Moreover, G intersects all the dense sets by construction. $\square$

This is really just the proof of the Baire category theorem.

§22.3 Splitting posets

This is very important: *we are interested in $\mathbb{P} \in M$ such that if $G \subseteq \mathbb{P}$ is an M-generic then $G \notin M$.*

Definition 22.7. A partial order $\mathbb{P}$ is **splitting** if for all $p \in \mathbb{P}$, there exists $q, r \le p$ such that $q \perp r$.

Exercise 22.8. Suppose $\mathbb{P}$ is splitting. Then if F is a filter such that $F \subseteq \mathbb{P}$ and $F \in M$, then $\mathbb{P} \setminus F$ is dense in $\mathbb{P}$.

Proof. Consider $p \notin \mathbb{P} \setminus F \iff p \in F$. Then there exists $q, r \le p$ which are not compatible. Since F is a filter it cannot contain both; we must have one of them outside F, say q. Hence every element of $p \in \mathbb{P} \setminus (\mathbb{P} \setminus F)$ has an element $q \le p$ in $\mathbb{P} \setminus F$. That's enough to prove $\mathbb{P} \setminus F$ is dense. $\square$

Of note is the case that $G \subseteq \mathbb{P}$ is an M-generic. We must have $G \notin M$ in that case. *This is very important – do not forget this fact!*

§22.4 Defining the generic extension

Definition 22.9. Suppose M is a transitive model of ZFC, $\mathbb{P} = (P, \le) \in M$ is a partial order, and $G \subseteq \mathbb{P}$ is M-generic. We define the **$\mathbb{P}$-names** recursively by

$$\begin{aligned} \text{Name}_0 &= \varnothing \\ \text{Name}_{\alpha+1} &= \mathcal{P}(\text{Name}_\alpha \times \mathbb{P}) \\ \text{Name}_\lambda &= \bigcup_{\alpha<\lambda} \text{Name}_\alpha. \end{aligned}$$

Finally, $\text{Name} = \bigcup_\alpha \text{Name}_\alpha$.

Definition 22.10. For $\tau \in \text{Name}$, let $\text{rank}(\tau)$ be the least α such that $\tau \in \text{Name}_\alpha$. We define the **interpretation** of τ, denote τ^G, using the transfinite recursion

$$\tau^G = \left\{ \sigma^G \mid \langle \sigma, p \rangle \in \tau \text{ and } p \in G \right\}.$$

Example 22.11
Let us compute

$$\begin{aligned}\text{Name}_0 &= \varnothing \\ \text{Name}_1 &= \mathcal{P}(\varnothing \times \mathbb{P}) \\ &= \{\varnothing\} \\ \text{Name}_2 &= \mathcal{P}(\{\varnothing\} \times \mathbb{P}) \\ &= \mathcal{P}\left(\{\langle \varnothing, p\rangle \mid p \in \mathbb{P}\}\right).\end{aligned}$$

Compare the corresponding von Neuman universe.

$$V_0 = \varnothing, \; V_1 = \{\varnothing\}, \; V_2 = \{\varnothing, \{\varnothing\}\}.$$

Example 22.12
For $\tau = \{\varnothing\}$, $\tau^G = \varnothing$.
Now suppose

$$\tau = \{(\varnothing, p_1), (\varnothing, p_2), \dots (\varnothing, p_n), \}.$$

Then

$$\tau^G = \{\varnothing \mid \langle \varnothing, p\rangle \in \tau \text{ and } p \in G\} = \begin{cases} \{\varnothing\} & \text{if some } p_i \in G \\ \varnothing & \text{otherwise.} \end{cases}$$

So under interpretation, we get V_2 back. In fact, we have in general that

$$\left\{\tau^G \mid \tau \in \text{Name}_n\right\} = V_n$$

for any $n \in \mathbb{N}$.

Things change at Name_ω.

Example 22.13 (Rasiowa-Sikorski Lemma)
Let M be a countable transitive model. Let $\mathbb{P}$ be the partial order on finite binary sequences ordered by $\supseteq$; this is possible since M satisfies ZFC. This gives a binary tree starting with $1_\mathbb{P}$ as the empty sequence. This is as splitting of a poset as we can possibly get. A filter then corresponds to some "branch".

Then a generic G consists of an infinite branch down, which corresponds to an infinite binary sequence. This G is not in M since $\mathbb{P}$ is splitting.

Now this generic G has the property that every binary sequence occurs in G. This follows since the set of points "ends in 101010" is a dense set.

§22.5 Defining $M[G]$

Definition 22.14. Set $M[G] = \left\{\tau^G \mid \tau \in \text{Name}^M\right\}$.

Definition 22.15. For $x \in M$, define by transfinite recursion a name

$$\check{x} = \{\langle \check{y}, 1_\mathbb{P}\rangle \mid y \in x\}.$$

Moreover, we define another name

$$\dot{G} = \{\langle \check{p}, p\rangle \mid p \in \mathbb{P}\}.$$

§23 November 18, 2014

§23.1 Review of Names

Recall that we defined

$$\check{x} = \{\langle \check{y}, 1_{\mathbb{P}} \rangle \mid y \in x\}.$$

Example 23.1

Compute

$$\begin{aligned} \check{0} &= 0 \\ \check{1} &= \{\langle \check{0}, 1_{\mathbb{P}} \rangle\}. \end{aligned}$$

So

$$\begin{aligned} (\check{0})^G &= 0 \\ (\check{1})^G &= 1. \end{aligned}$$

In general, $(\check{x})^G = x$.

Basically, $\check{x}$ is just a copy of x where we add check marks and tag every element with $1_{\mathbb{P}}$.

Recall also that we define

$$\dot{G} = \{\langle \check{p}, p \rangle \mid p \in \mathbb{P}\}.$$

Thus

$$\begin{aligned} (\dot{G})^G &= \left\{ \sigma^G \mid \langle \sigma, p \rangle \in \dot{G} \wedge p \in G \right\} \\ &= \left\{ (\check{p})^G \mid \langle \check{p}, p \rangle, p \in \mathbb{P} \right\} \\ &= \{p \mid p \in G\} \\ &= G. \end{aligned}$$

Note that $\check{x}, \dot{G} \in M$.

Exercise 23.2. Show that $\operatorname{rank} \sigma^G \le \text{n-rank}(\sigma)$ for all names σ in M.

All the names live inside M. Some names, when interpreted, live inside M. But you can find names which when interpreted which fall outside M; an example is $\dot{G}$.

The whole point of this construction is that G lives outside M.

§23.2 Filters of Transitive Models

Lemma 23.3

Suppose M is a transitive model of ZFC and $\mathbb{P} \in M$ is a partial order. Let $G \subseteq \mathbb{P}$ is a filter. Then

(1) $M \subseteq M[G]$

(2) $G \in M[G]$

(3) $M[G]$ is transitive.

(4) The ordinals of M are the same as the ordinals of $M[G]$.

Proof. For (1), note that $x = (\widehat{x})^G \in M[G]$. For (2), note that $G = (\dot{G})^G \in M[G]$.

For (3), consider $x \in M[G]$ and $y \in x$. Let $\sigma \in \text{Name}^M$ such that $x = \sigma^G$. Then

$$y \in \sigma^G = \left\{ \tau^G \mid \langle \tau, p \rangle \in \sigma \wedge p \in G \right\}.$$

Hence $y = \tau^G$ for some τ. We have $\tau \in \sigma \in M$, so transitivity of M gives $\tau \in M$. Thus $y = \tau^G \in M[G]$.

For (4), by absoluteness the ordinals of M are precisely the ordinals in the universe V which live inside M. In other words,

$$(\text{On})^M = \text{On}^V \cap M.$$

Analogously

$$(\text{On})^{M[G]} = \text{On}^V \cap M[G].$$

Since $M \subsetneq M[G]$ we have $\text{On} \cap M \le \text{On} \cap M[G]$. But we also know that for any $\sigma \in \text{Name}^M$ we have

$$\text{rank}(\sigma^G) \le \text{n-rank}(\sigma)$$

and so the inequality is sharp. $\square$

Lemma 23.4

Suppose M is a transitive model of ZFC and $\mathbb{P} \in M$ is a partial order. Let $G \subseteq \mathbb{P}$ is a filter. Then

$$M[G] \vDash \text{ZF} - (\text{Comprehension} + \text{Replacement} + \text{Powerset}).$$

The missing axioms (including AC) will be recovered when we assume G is in fact a generic, not just a filter.

Proof. Extensionality and Foundation follow from the fact that $M[G]$ is transitive. Emptyset and Infinity get inherited from M, since $M \subseteq M[G]$.

For Pairing, suppose $x, y \in M[G]$. Let $\sigma_1, \sigma_2 \in \text{Name}^M$ be such that $\sigma_1^G = x$ and $\sigma_2^G = y$. We seek a $\sigma \in \text{Name}^M$ such that $\sigma^G = \left\{ \sigma_1^G, \sigma_2^G \right\}$; the choice

$$\sigma = \{ \langle \sigma_1, 1_{\mathbb{P}} \rangle, \langle \sigma_2, 1_{\mathbb{P}} \rangle \}$$

works. And this is why we're happy; $1_{\mathbb{P}}$ is always in the generic. (Note that we used Pairing in M.)

Finally, we show Union. Let $\sigma^G = x \in M[G]$; we seek a σ' such that $\sigma'^G = \cup \sigma^G$. Now

$$\cup \sigma^G = \cup \left\{ \tau^G \mid \langle \tau, p \rangle \in \sigma \wedge p \in G \right\}. = \left\{ x \mid x \in \tau^G \text{ for some } \langle \tau, p \rangle \in \sigma, p \in G \right\}.$$

Now let

$$\begin{aligned} \sigma' = \{ \langle \overline{\tau}, r \rangle \mid & \exists \tau \exists p, q \in \mathbb{P} \text{ such that} \\ & \langle \overline{\tau}, p \rangle \in \tau \wedge \\ & \langle \tau, q \rangle \in \sigma \wedge \\ & r \le p, q \}. \end{aligned}$$

You can check that this works. $\square$

§23.3 Using the Generic Condition

So far we have assumed that

(a) M is a transitive model of ZFC.

(b) $G \subseteq \mathbb{P} \in M$ is a filter. Assuming G exists, we have the bunch of axioms proven above.

(c) By further assuming M is countable, we showed that an M-*generic* filter G exists for any partial order $\mathbb{P}$. By taking $\mathbb{P}$ to be splitting, we deduced that $G \notin M$.

We want to now show that $M[G]$ implies PowerSet, Comprehension, Replacement, AC; this will give $M[G] \vDash$ ZFC. Then by carefully choosing G we will try to force $M[G] \vDash \neg$CH.

Suppose we want to show Comprehension holds in $M[G]$. Let $\sigma^G \in M[G]$ and $\phi(x_0, x_1, \dots, x_n)$ is a formula in LST. Let $\tau_1^G, \tau_2^G, \dots, \tau_n^G$ be parameters. We wish to show

$$M[G] \vDash \exists y \left(y = \left\{ x \mid x \in \sigma^G \text{ and } \varphi[x, \tau_1^G, \dots, \tau_n^G] \right\} \right).$$

To build the appropriate name y, we need to be able to determine

$$M[G] \vDash \varphi[x, \tau_1^G, \dots, \tau_n^G]$$

in order to do anything. So we have to use the truths in M (which can't see G at all) in order to get (or at least approximate) truths in $M[G]$. As G varies, the truths in $M[G]$ vary, and somehow M can't see these.

We're running a bit out of time because I asked some intuition questions (some of the answers which I filled in retroactively to the last lecture), so I'll just state the big theorem.

Theorem 23.5 (Fundamental Theorem of Forcing)
Suppose M is a transitive model of ZF. Let $\mathbb{P} \in M$ be a poset, and $G \subseteq \mathcal{P}$ is an M-generic filter. Then,

(1) Consider $\sigma_1, \dots, \sigma_n \in \text{Name}^M$, Then

$$M[G] \vDash \varphi[\sigma_1^G, \dots, \sigma_n^G]$$

if and only if there exists a condition $p \in G$ such that p *forces* the sentence $\varphi(\sigma_1, \dots, \sigma_n)$. We denote this by $p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$.

(2) This forcing relation is (uniformly) definable in M.

§24 November 20, 2014

Note: no class next Tuesday.

Today we will define the forcing relation

$$p \Vdash^M_{\mathbb{P}} \phi(\sigma_1, \dots, \sigma_n)$$

where $p \in \mathbb{P}$ and $\phi \in \text{LST}$ in M.

§24.1 Motivation

Recall Cohen's *Fundamental Theorem of Forcing* from the previous lecture.

Hope: in M we define a semantic relation $\#^M_{\mathbb{P}}$ such that for $p \in \mathbb{P}$ and $\sigma_1, \dots, \sigma_n \in \text{Name}^M$ the following are equivalent:

(1) $p \#^M_{\mathbb{P}} \varphi(\sigma_1, \dots, \sigma_n)$

(2) for every M-generic $G \subseteq \mathbb{P}$ if $p \in G$ then $M[G] \vDash \varphi[\sigma_1^G, \dots, \sigma_n^G]$.

Our goal is to show $\#$ is $\Vdash$.

Compare the completeness theorem: Recall the semantic notation of logical consequence $\vDash$: we write $\Gamma \vDash \varphi$ (where $\Gamma \subseteq \text{LST}$) if any model M which satisfies Γ also satisfies φ. The sentences of Γ themselves are encoded as natural numbers. We're looking through all the models M; this is hence a Π_1-definable notion. Now the completeness theorem says that $\Gamma \vDash \phi$ if and only if $\Gamma \vdash \phi$ (i.e. there exists a proof, which can also be encoded as a natural number $\mathbb{N}$). The former is a Π_1 notion over V; the latter is a Σ_1 notion of $\mathbb{N}$.

This conversion is the power here. When we prove Fermat's Last Theorem in ZFC, we didn't go through every model of V; rather we simply wrote down the proof, which can be encoded in a natural number. Our hope is that we can do the same thing with the clause "for all generics $G \subseteq \mathbb{P}$".

§24.2 Semantics and Desired Conditions

We desire the following conditions on our $\Vdash$.

(1) Persistence: If $q \le_{\mathbb{P}} p$ and $p \Vdash \phi$ then $q \Vdash \phi$.

(2) Consistency: If $p \Vdash \phi$ then $p \nVdash \neg\phi$.

(3) Completeness (the interesting one): If $p \nVdash \phi$ then $\exists q \le_{\mathbb{P}} p$ such that $q \Vdash \neg\phi$. In other words, the set of conditions which force ϕ are dense.

Obviously $\#$ satisfies all these properties. In fact, we claim that along with the first part of the Fundamental Theorem of Forcing, this gives $\Vdash \cong \#$.

Proposition 24.1

Suppose we've defined a $\Vdash$ that satisfies the three relations above. Then part (1) of the Fundamental Theorem of Forcing implies

$$(p \Vdash \varphi \iff p \# \varphi).$$

Proof. First, suppose $p \Vdash \varphi$; we want to prove $p \# \varphi$. Assume for contradiction that $p \not\# \varphi$. Then there exists a M-generic $G \subseteq \mathbb{P}$ such that $p \in G$ and

$$M[G] \vDash \neg\phi[\sigma_1^G, \dots, \sigma_n^G].$$

Then by the Fundamental Theorem of Forcing there exists $q \in G$ so that

$$q \Vdash \neg\varphi(\sigma_1, \dots, \sigma_n).$$

But now since G is a filter we have some $r \le p, q$. Since $p \Vdash \varphi$ and $q \Vdash \neg\varphi$, Persistence gives $r \Vdash \varphi, \neg\varphi$ which is impossible.

Conversely, suppose $p \# \varphi$. We wish to show $p \Vdash \varphi$. Suppose not, so $p \nVdash \varphi$. By Completeness, there exists $q \le p$ such that $q \Vdash \neg\phi$. Let G be an M-generic such that $q \in G$. Thus

$$M[G] \vDash \neg\varphi[\sigma_1^G, \dots, \sigma_n^G].$$

But $p \ge q \implies p \in G$ (by upwards closure), and then $M[G] \vDash \varphi[\sigma_1^G, \dots, \sigma_n^G]$. $\square$

§24.3 Defining the Relation

Now that we're done with that tautology, we need to show $\Vdash$ satisfies the Fundamental Theorem of Forcing as well as the three properties Persistence, Consistency, Completeness.

We'll go by induction on the formula complexity. It turns out in this case that the atomic formula (base cases) are hardest and themselves require induction on ranks.

For some motivation, let's consider how we should define $p \Vdash \tau_1 \in \tau_2$ given that we've already defined $p \vDash \tau_1 = \tau_2$. We need to ensure this holds iff

$$\forall M\text{-generic } G \text{ with } p \in G: \ M[G] \vDash \tau_1^G \in \tau_2^G.$$

So it suffices to ensure that any generic $G \ni p$ hits a condition q which forces τ_1^G to *equal* a member τ^G of τ_2^G. In other words, we want to choose the definition of $p \Vdash \tau_1 \in \tau_2$ to hold if and only if

$$\{q \in \mathbb{P} \mid \exists \langle \tau, r \rangle \in \tau_2 \, (q \le r \wedge q \Vdash (\tau = \tau_1))\}$$

is dense below in p. In other words, if the set is dense, then the generic must hit q, so it must hit r, meaning that $\langle \tau_r \rangle \in \tau_2$ will get interpreted such that $\tau^G \in \tau_2^G$, and moreover the $q \in G$ will force $\tau_1 = \tau$.

Now let's write down the definition... In what follows, the $\Vdash$ omits the M and $\mathbb{P}$.

Definition 24.2. Let M be a countable transitive model of ZFC. Let $\mathbb{P} \in M$ be a partial order. For $p \in \mathbb{P}$ and $\varphi(\sigma_1, \dots, \sigma_n)$ a formula in LST, we write $\tau \Vdash \varphi(\sigma_1, \dots, \sigma_n)$ to mean the following, defined by induction on formula complexity plus rank.

(1) $p \Vdash \tau_1 = \tau_2$ means

(i) For all $\langle \sigma_1, q_1 \rangle \in \tau_1$ the set

$$D_{\sigma_1, q_1} \overset{\text{def}}{=} \{r \mid r \le q_1 \to \exists \langle \sigma_2, q_2 \rangle \in \tau_2 \, (r \le q_2 \wedge r \Vdash (\sigma_1 = \sigma_2))\}.$$

is dense in p. (This encodes "$\tau_1 \subseteq \tau_2$".)

(ii) For all $\langle \sigma_2, q_2 \rangle \in \tau_2$, the set D_{σ_2, q_2} defined similarly is dense below p.

(2) $p \Vdash \tau_1 \in \tau_2$ means

$$\{q \in \mathbb{P} \mid \exists \langle \tau, r \rangle \in \tau_2 \, (q \le r \wedge q \Vdash (\tau = \tau_1))\}$$

is dense below p.

(3) $p \Vdash \varphi \wedge \psi$ means $p \Vdash \varphi$ and $p \Vdash \psi$.

(4) $p \Vdash \neg\varphi$ means $\forall q \le p$, $q \nVdash \varphi$.

(5) $p \Vdash \exists x \varphi(x, \sigma_1, \dots, \sigma_n)$ means that the set

$$\{q \mid \exists \tau \, (q \Vdash \varphi(\tau, \sigma_1, \dots, \sigma_n)\}$$

is dense below p.

This is definable in M! All we've referred to is $\mathbb{P}$ and names, which are in M. (Note that being dense is definable.) Actually, in parts (3) through (5) of the definition above, we use induction on formula complexity. But in the atomic cases (1) and (2) we are doing induction on the ranks of the names.

§24.4 Consequences of the Definition

Exercise 24.3. Show that

(1) If $p \Vdash \varphi$ and $q \le p$ then $q \Vdash \varphi$.

(2) If $\{q \mid q \Vdash \varphi\}$ is dense below p then $p \Vdash \varphi$.

These are just inductions on the five parts of the definition. The first guy is Persistence; the second is a sort of converse. Consistency is immediate from the definition (take $q = p$ in the definition). We can use this to establish Completeness as a corollary.

Corollary 24.4

If $p \nVdash \varphi$ then for some $\overline{p} \le p$ we have $\overline{p} \Vdash \neg\varphi$.

Proof. By the exercise $\{q \mid q \Vdash \varphi\}$ is not dense below p, meaning for some $\overline{p} \le p$, every $q \le \overline{p}$ gives $q \nVdash \varphi$. By the definition of $p \vDash \neg\varphi$, we have $\overline{p} \vDash \neg\varphi$. $\square$

Now we are in the position to prove the Fundamental Theorem of Forcing. We have already shown (2) of the Fundamental Theorem. Next lecture we will prove (1).

§25 December 2, 2014

Today we'll be doing the independence of CH.

Reproduced here again is the fundamental theorem of forcing.

> Suppose M is a transitive model of ZF. Let $\mathbb{P} \in M$ be a poset, and $G \subseteq \mathcal{P}$ is an M-generic filter. Then,
>
> (1) Consider $\sigma_1, \dots, \sigma_n \in \text{Name}^M$, Then
> $$M[G] \vDash \varphi[\sigma_1^G, \dots, \sigma_n^G]$$
> if and only if there exists a condition $p \in G$ such that p *forces* the sentence $\varphi(\sigma_1, \dots, \sigma_n)$. We denote this by $p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$.
>
> (2) This forcing relation is (uniformly) definable in M.

Here "uniformly" means that the definition can be written down without relying on properties of M; in other words, there is some fixed definition that we can run in more models.

§25.1 Forcing tells us that $M[G]$ satisfies ZF

Theorem 25.1

Suppose M is a transitive model of ZF. Let $\mathbb{P} \in M$ be a poset, and $G \subseteq \mathcal{P}$ is an M-generic filter. Then
$$M[G] \vDash \text{ZF}.$$
Moreover if M satisfies Choice, so does $M[G]$.

Proof. (Partial) The easy stuff is a lemma from the previous lecture. We always have $M[G]$ satisfies Extensionality and Foundation. Also check it satisfies EmptySet, Infinity, Pairing, Union. (We did this in an earlier lecture). Up to here we did not need the Fundamental Theorem of Forcing.

The issue is different with Comprehension because we need to actually understand when a formula is true in $M[G]$. Let's do Comprehension.

Proof of Comprehension. Suppose $\sigma^G, \sigma_1^G, \dots, \sigma_n^G \in M[G]$ are a set and parameters, and $\varphi(x, x_1, \dots, x_n)$ is an LST formula. We want to show that the set
$$A = \left\{x \in \sigma^G \mid M[G] \vDash \varphi[x, \sigma_1^G, \dots, \sigma_n^G]\right\}$$
is in $M[G]$.

Note that every element of σ^G is of the form ρ^G for some $\rho \in \text{dom}(\sigma)$ (since σ is a bunch of pairs of names and p's). So by the Fundamental Theorem of Forcing, we may write
$$A = \left\{\rho^G \mid \rho \in \text{dom}(\sigma) \text{ and } \exists p \in G \left(p \Vdash \rho \in \sigma \wedge \varphi(\rho, \sigma_1, \dots, \sigma_n)\right)\right\}.$$
To show $A \in M[G]$ we have to write down a τ such that the name τ^G coincides with A. We claim that
$$\tau = \{\langle \rho, p\rangle \in \text{dom}(\sigma) \times \mathbb{P} \mid p \Vdash \wedge \varphi(\rho, \sigma_1, \dots, \sigma_n)\}$$
is the correct choice. It's actually clear that $\tau^G = A$ by construction; the "content" is showing that τ is in actually a name of M, which follows from Comprehension in M.

So really, the point of the Fundamental Theorem of Forcing is just to let us write down this τ; it lets us show that τ is in Name^M without actually referencing G. ■

Everything else is similar. □

§25.2 Forcing $V \neq L$ is really easy

Given M, we are now going to pick a partial order such that $M[G]$ has $V \neq L$. Note the contrast here: given a ZFC model M,

- We could construct L^M by running the definition of L in M, obtaining an "internal model" $L^M \vDash \mathrm{ZFC} + V = L$. (By "internal" I mean L^M lives inside M)
- We are now going to construct an *external* model $M[G]$ for which $V \neq L$.

Note that this is one step on the way to CH; since $V = L$ along with ZFC implies CH, this is the first necessary step.

Let $\mathbb{P} \in M$ be a splitting poset like the **infinite complete binary tree** $\mathbb{P} = ({}^{<\omega}2, \supseteq)$ (look this up).

Theorem 25.2

Let M be a countable transitive model of ZFC. Let $\mathbb{P} \in M$ be *any* splitting poset, and let $G \subseteq \mathbb{P}$ be M-generic. Then $M[G] \vDash (V \neq L)$.

Proof. Since $\mathbb{P}$ is splitting, $G \notin M$, so there are elements of $M[G]$ not in M.

Since L has a Σ_1 definition, we have

$$L^{M[G]} = L^M$$

the latter which is contained in M. So $L^{M[G]}$ is contained in M and hence cannot encompass all of $M[G]$. Hence $M[G]$ satisfies the sentence $\exists x (x \notin L)$, QED. □

You can do this even more dramatically. Given any $L_\lambda \vDash \mathrm{ZFC}$, take $\mathbb{P}$ be a splitting poset; then $L_\lambda[G]$ does what we want. Hence we've shown that if M is a countable transitive model of ZFC then we get an $M[G]$ which is a countable transitive model of ZFC and $V \neq L$. We'll strengthen this to the following result.

Theorem 25.3

Suppose ZFC is consistent. Then so is $\mathrm{ZFC} + (V \neq L)$.

The proof will use the Compactness Theorem.

Proof. Let N be a model of ZFC (not necessarily transitive or even well-founded). We want to build an N' obeying $\mathrm{ZFC} + (V \neq L)$. By the Compactness Theorem it suffices to show that for any finite fragment F of ZFC, $F + (V \neq L)$ has a model M_F.

Issue: N could be ill-founded but the Fundamental Theorem of Forcing is phrased in terms of transitive models, so we cannot just take the Mostowski collapse. However, we can just drop into N. Let F be a fragment; let F' be a sufficiently bigger fragment of ZFC which ensures that $M_F[G] \vDash +(V \neq L)$. By reflection there exists a λ with $V_\lambda^N \vDash F'$. Now N thinks V_λ^N is transitive, so we can take an elementary substructure M_F. Even though M_F might be ill-founded, it's still a model. Use forcing:

$$M_F \vDash F' \implies M_F[G] \vDash F + (V \neq L).$$

Using compactness, from M_F for every F then we get N'. □

§25.3 Forcing ZFC + ¬CH

Starting with a countable transitive model M, pick $\mathbb{P}$ in M such that if $G \subseteq \mathbb{P}$ is M-generic, then $M[G] \vDash \neg\text{CH}$.

We want to choose $\mathbb{P} \in M$ such that $(\aleph_2)^M$ many real numbers appear. However, we need to make sure that $(\aleph_2)^M \mapsto (\aleph_2)^{M[G]}$ doesn't get collapsed. In other words, we want to make sure that

$$(\aleph_2)^{M[G]} = (\aleph_2)^M .$$

Then, $M[G]$ will satisfy the sentence "there are at least $(\aleph_2)^M$ many real numbers".

Recall the earlier situation where we set $\mathbb{P}$ to be the infinite complete binary tree; its nodes can be thought of as partial functions $n \to 2$ where $n < \omega$. Then G itself is a path down this tree; i.e. it can be encoded as a total function $G : \omega \to 2$. Thus it corresponds to a real number $G \notin M$. Now what we'd like to do is add in tons of reals by considering reals as subsets of $\mathbb{N}$.

Consider in M the following poset:

$$\text{Add}\left(\omega_2, \omega\right) \overset{\text{def}}{=} \left(\left\{p : \omega_2 \times \omega \to 2, \text{dom}(p) < \omega\right\}, \supseteq\right)$$

these elements (conditions) are "partial functions": we take some finite subset of $\omega \times \omega_2$ and map it into $2 = \{0, 1\}$. Moreover, $p \le_{\mathbb{P}} q$ if $\text{dom}(p) \supseteq \text{dom}(q)$ and the two functions agree over $\text{dom}(q)$. We claim that this adds ω_2 many reals.

Let $G \subseteq \text{Add}(\omega_2, \omega)$ be an M-generic. We claim that, like in the binary case, G can be encoded as a function $\omega_2 \times \omega \to 2$. To see this, consider $\alpha \in \omega_2$ and $n \in \omega$; we have the dense set

$$D_{\alpha,n} = \{p \in \text{Add}(\omega_2, \omega) \mid (\alpha, n) \in \text{dom}(p)\}$$

(this is obviously dense, given any p add in (α, n) if it's not in there already). So G hits this dense set, meaning that for every (α, n) there's a function in G which defines it. Using the fact that G is upwards closed and a filter, we may as before we may interpret G as a function $\omega_2 \times \omega \to 2$.

For a fixed α define

$$G_\alpha = \{n \mid G\left(\langle \alpha, n\rangle\right) = 0\} \in \mathcal{P}(\mathbb{N})$$

which is a real number for each $\alpha < \omega_2$.

Claim 25.4. Let $\alpha, \beta \in \omega_2$. Then $G_\alpha \neq G_\beta$ for any $\alpha \neq \beta$.

Proof. We claim the following set is dense:

$$D = \left\{q \mid \exists n \in \omega : q\left((\alpha, n)\right) \neq q\left((\beta, n)\right)\right\}.$$

This is pretty easy to see. Consider $p \in \text{Add}(\omega_2, \omega)$, Then you can find an n such that neither (α, n) nor (β, n) is defined, just because $\text{dom}(p)$ is finite. Then you make p' as p plus $p'((\alpha, n)) = 1$ and $p'((\beta, n)) = 0$. Hence the set is dense.

Since G is an M-generic it hits this dense set D. Hence $G_\alpha \neq G_\beta$. $\square$

So, start with a countable transitive model M of ZFC. Let

$$\mathbb{P} = \left(\text{Add}(\omega_2, \omega)\right)^M$$

and let $G \subseteq \mathbb{P}$ be an M-generic. Then G adds $(\aleph_2)^M$ many new real numbers. Why? Note G itself is an element of $M[G]$ (interpret $\dot{G}$), and hence each G_α is an element of $M[G]$, but from every G_α we can construct a new real.

§26 December 4, 2014

We're trying to force not CH now!

Let M be a countable transitive model of ZFC, and we let $\mathbb{P}$ be the partial order $\mathbb{P} = (\text{Add}(\omega, \omega_2))^M$. We showed that $M[G]$ contains $(\omega_2)^M$ many new subsets of ω. So it just remains to show that

$$(\omega_2)^{M[G]} = (\omega_2)^M.$$

In fact, we will show that M satisfies "κ is a cardinal" if and only if $M[G]$ satisfies the same sentence. This will entirely resolve the problem of CH, since we can just climb the chain of ordinals; this will cause all the cardinals to match up.

§26.1 The Countable Chain Condition

Definition 26.1. A poset $\mathbb{P}$ has the **κ-chain condition** (where κ is a cardinal) if all antichains in $\mathbb{P}$ have size less than κ. The special case $\kappa = \aleph_1$ is called the **countable chain condition**.

Here are *antichain* means that no two pairs of elements are compatible (not comparable, like the usual meaning).

We are going to show that if the poset has the κ-chain condition then it preserves all cardinals greater than κ. In particular, the countable chain condition will show that $\mathbb{P}$ preserves all the cardinals. Then, we'll show that $\text{Add}(\omega, \omega_2)$ does indeed have this property. This will complete the proof.

§26.2 Possible Values Argument

The following argument is important enough that we isolate it separately.

Lemma 26.2 (Possible Values Argument)

Suppose M is a transitive model of ZFC and $\mathbb{P}$ is a partial order such that $\mathbb{P}$ has the κ-chain condition in M. Let $X, Y \in M$ and let

$$f : X \to Y$$

be some function in $M[G]$, but not necessarily in M. Then there exists a function $F \in M$ such that for any $x \in X$, we have

$$f(x) \in F(x)$$

and

$$|F(x)|^M < \kappa.$$

Intuitively, F tells us that we can narrow down the possible values of f to a set of size κ .

Proof. Let $\dot{f}$ be a name for f, hence $\dot{f}^G = f$. Similarly, let $\check{X}$ and $\check{Y}$ be the canonical names for X and Y. By the Fundamental Theorem of Forcing, we have that for some p,

$$p \Vdash \exists \text{ function } \hat{f} : \check{X} \to \check{Y}$$

We work in M now. For each $x \in X$, we let $A(x)$ be a maximal set of pairwise incompatible conditions conditions $q \le_{\mathbb{P}} p$ such that

$$\forall q \in A(x) \exists y \in Y \left(q \Vdash \dot{f}(\check{x}) = \check{y} \right).$$

Note this uses the Axiom of Choice. What this is doing is as follows. We let q_0 be a guy which forces $f(x)$ to be some y_0, q_1 to be a guy which forces $f(x)$ to be some other y_1, and so on. Then let

$$F(x) = \{y \in Y \mid \exists q \in A(x) : q \Vdash f(\check{x}) = \check{y}\}.$$

The chain condition means that $|F(x)|^M < \kappa$. So now we just have to show we got all possible values.

Suppose $f(x) = y$, meaning $(\dot{f})^G(x) = y$. Let $q' \in G$ be such that

$$q' \Vdash (\dot{f})(\check{x}) = \check{y}.$$

WLOG $q' \le p$. Since $A(x)$ is a maximal, there must exist $q \in A(x)$ such that q and q' are compatible. Let $r \le q, q'$ accordingly. Hence

$$r \Vdash \dot{f}(\check{x}) = \check{y}.$$

But $q \Vdash \dot{f}(\check{x}) = \check{z}$ for some $z \in Y$. Thus $f(x) = y \in F(x)$. □

§26.3 Preserving Cardinals

Definition 26.3. For M a transitive model of ZFC and $\mathbb{P} \in M$ a poset, we say $\mathbb{P}$ **preserves cardinals** if $\forall G \subseteq \mathbb{P}$ an M-generic, the model M and $M[G]$ agree on the sentence "κ is a cardinal" for every κ.

In the same way we will talk about $\mathbb{P}$ preserving cofinalities, et cetera.

Exercise 26.4. Let M be a transitive model of ZFC. Let $\mathbb{P} \in M$ be a poset. Show that the following are equivalent for each λ:

(1) $\mathbb{P}$ preserves cofinalities less than or equal to λ.

(2) $\mathbb{P}$ preserves regular cardinals less than or equal to λ.

Moreover the same holds if we replace "less than or equal to" by "greater than or equal to".

Thus, to show that $\mathbb{P}$ preserves cardinality and cofinalities it suffices to show that $\mathbb{P}$ preserves regularity.

Theorem 26.5

Suppose M is a transitive model of ZFC, and $\mathbb{P} \in M$ is a poset. Suppose M satisfies the sentence "$\mathbb{P}$ has the κ chain condition and κ is regular". Then $\mathbb{P}$ preserves cardinals and cofinalities greater than or equal to κ.

Proof. It suffices to show that $\mathbb{P}$ preserves regularity greater than or equal to κ. Consider $\lambda > \kappa$ which is regular in M, and suppose for contradiction that λ is not regular in $M[G]$. That's the same as saying that there is a function $f \in M[G]$, $f : \overline{\lambda} \to \lambda$ cofinal, with $\overline{\lambda} < \lambda$. Then by the Possible Values Argument, there exists a function $F \in M$ from $\overline{\lambda} \to \mathcal{P}(\lambda)$ such that $f(\alpha) \in F(\alpha)$ and $|F(\alpha)|^M < \kappa$ for every α.

Now we work in M again. Note for each $\alpha \in \overline{\lambda}$, $F(\alpha)$ is bounded in λ since λ is regular in M and greater than $|F(\alpha)|$. Now look at the function $\overline{\lambda} \to \lambda$ in M by just

$$\alpha \mapsto \cup F(\alpha) < \lambda.$$

This is cofinal in M, contradiction. □

§26.4 Infinite Combinatorics

In particular, if $\mathbb{P}$ has the countable chain condition then $\mathbb{P}$ preserves all the cardinals (and cofinalities). Therefore, it remains to show that $\text{Add}(\omega, \omega_2)$ satisfies the countable chain condition. And this is going to be infinite combinatorics.

Definition 26.6. Suppose C is an uncountable collection of finite sets. C is a **Δ-system** if there exists a **root** R with the condition that for any distinct X and Y in C, we have $X \cap Y = R$.

Lemma 26.7 (Δ-System Lemma)
Suppose C is an uncountable collection of finite sets. Then $\exists \overline{C} \subseteq C$ such that

(1) $\overline{C}$ is uncountable.

(2) $\overline{C}$ is a Δ-system.

Proof. There exists an integer n such that C has uncountably many guys of length n. So we can throw away all the other sets, and just assume that all sets in C have size n.

We now proceed by induction on n. The base case $n = 1$ is trivial, since we can just take $R = \varnothing$. For the inductive step we consider two cases.

First, assume there exists an $a \in C$ contained in uncountably many $F \in C$. Throw away all the other guys. Then we can just delete a, and apply the inductive hypothesis.

Now assume that for every a, only countably many members of C have a in them. We claim we can even get a $\overline{C}$ with $R = \varnothing$. First, pick $F_0 \in C$. It's straightforward to construct an F_1 such that $F_1 \cap F_0 = \varnothing$. And we can just construct $F_2, F_3, \dots$ □

Lemma 26.8
For all κ, $\text{Add}(\omega, \kappa)$ satisfies the countable chain condition.

Proof. Assume not. Let

$$\{p_\alpha : \alpha < \omega_1\}$$

be an antichain. Let

$$C = \{\text{dom}(p_\alpha) : \alpha < \omega_1\}.$$

Let $\overline{C} \subseteq C$ be such that $\overline{C}$ is uncountable, and $\overline{C}$ is a Δ-system which root R. Then let

$$B = \{p_\alpha : \text{dom}(p_\alpha) \in R\}.$$

Each $p_\alpha \in B$ is a function $p_\alpha : R \to \{0, 1\}$, so there are two that are the same. □

§26.5 Finishing Off

Let's wrap this all up.

Theorem 26.9
Let M be a countable transitive model of ZFC. Then there exists a generic extension

$$M[G] \vDash \text{ZFC} + \neg\text{CH}.$$

Proof. Let $\mathbb{P} = (\mathrm{Add}(\omega, \omega_2))^M$. Let $G \subseteq \mathbb{P}$. Then $M[G] \vDash 2^\omega > (\omega_2)^M$. But we also know that

$$(\omega_2)^{M[G]} = (\omega_2)^M.$$

Thus

$$M[G] \vDash 2^\omega \geq \aleph_2$$

hence

$$M[G] \vDash \mathrm{ZFC} + \neg\mathrm{CH}.$$

□

With our work before we showed that we don't need the countable transitive model because if we just have any old model N of ZFC, we can construct a countable transitive model internally.

Hence $V = L$ and CH are both totally independent of ZFC.

§26.6 Concluding Remark

You can use forcing to prove even more things. One can construct models for Suslin's Hypothesis, its negation, $2^\omega = \aleph_{17}$, and so on.

Next semester, we'll study large candinals as a system of new axioms, and these settle questions like $V = L$, and the HOD dichotomy.

OK, fine, a teaser.

Definition 26.10. A cardinal κ is **measurable** if there exists an elementary embedding (i.e. preserving truth or satisfaction)

$$j : V \to M$$

where M is a transitive class, j is not the identity, and κ is the first ordinal moved.

This κ is very powerful and very big. It is regular, inaccessible, ... Moreover, the definition can be made first order.

Theorem 26.11 (Scott)
Assume ZFC plus the sentence "there is a measurable cardinal κ". Then $V \neq L$.

Proof. Assume for contradiction that $V = L$. Let κ be the least measurable cardinal in $V = L$. Take $j : L = V \to M$ witness that κ is measurable.

But $V \vDash (V = L)$, $M \vDash (V = L)$, yet M is transitive. That means M has to be L. Since L satisfies "κ is the least measurable cardinal" it follows that L also satisfies "$j(\kappa)$ is the least measuarble cardinal". But $\kappa < j(\kappa)$. Everything breaks. □