Lecture 1: Introduction and Axioms
January 19, 2009

1 Introduction

Remark. Generally speaking, there are two sorts of mathematical theories: those, like number theory, that seek to describe and explore some particular structure; and those, like group theory, that seek to generalize structures found elsewhere. In this respect, we conceive of set theory as being more like number theory: it seeks to describe the cumulative hierarchy of sets.

The *cumulative hierarchy of sets* begins with just the empty set; then we use the power set operator to build further levels.

$$V_0 = \emptyset$$
$$V_{n+1} = \mathcal{P}(V_n).$$

Each of these stages is finite. We can then construct a *limit stage* as follows:

$$V_\omega = \bigcup_{n \in \mathbb{N}} V_n.$$

V_ω is known as the collection of *hereditarily finite sets*: any set in V_ω is finite, and so are its elements, and the elements of its elements, and the elements of elements of elements... and so on.

We also want to be able to deal with infinite sets—in fact, set theory was introduced by Cantor in the 1880s partly to deal with infinity in the context of real analysis. So we can introduce

$$V_{\omega+1} = \mathcal{P}(V_\omega)$$

and so on, leading to the notion of *transfinite ordinals*. Much more will be said about this in time.

So set theory is about saying as much as possible about this cumulative hierarchy of sets; characterizing both the "height" (ordinals) and "width" (power set operator).

2 Zermelo-Frankel Axioms

Remark. This axiomatization of set theory was developed first by Zermelo in 1908 and extended by Frankel and Skolem in 1922/3. The Zermelo-Frankel axioms with the Axiom of Choice are often abbreviated "ZFC". This is a first-order theory with $=$ and $\in$ the only non-logical symbols. The axioms are as follows.

1. Extensionality.

$$\forall x.\forall y.(\forall z.z \in x \Leftrightarrow z \in y) \Rightarrow x = y.$$

Two sets are equal if they have the same elements.

2. Pairing.

$$\forall x.\forall y.\exists z.\forall w.(w \in z \Leftrightarrow (w = x \vee w = y)).$$

We can form a set with two given sets as elements (i.e. an unordered pair).

Note that we can now form "ordered pairs" by identifying the ordered pair (x, y) with the set $\{\{x\}, \{x, y\}\}$; note that the set $\{x\}$ exists by the axiom of Pairing (pair x with itself).

3. Union.

$$\forall x.\exists y.\forall z.z \in y \Leftrightarrow (\exists w.w \in x \wedge z \in w).$$

For every set x there exists a set y (which we will abbreviate $\bigcup x$) whose elements are exactly the elements of the elements of x.

4. Power set.

$$\forall x.\exists y.\forall z.z \in y \Leftrightarrow z \subseteq x.$$

For every set x there exists a set y (abbreviated $\mathcal{P}(x)$) whose elements are precisely the subsets of x. Note that we use $z \subseteq x$ as an abbreviation for $\forall w.w \in z \Rightarrow w \in x$.

5. Comprehension. If φ is a first-order formula which does not contain y free, then

$$\forall x.\exists y.\forall z.z \in y \Leftrightarrow (z \in x \wedge \varphi(z)).$$

Note that this is an axiom *schema* representing an infinite number of axioms, one for each φ. This says that we may "carve out" those elements of x satisfying φ to form a new set y.

Initially, this axiom was expressed by Frege as

$$\exists y.\forall z.z \in y \Leftrightarrow \varphi(z),$$

now known as the "naïve extension principle". In 1902 Russell showed that this led to his now-famous paradox: if we let $\varphi(z) = z \notin z$, then the naïve extension principle says there is some set y such that for all z, $z \in y \Leftrightarrow z \notin z$—but if we take z to be y, this results in the absurd conclusion that $y \in y \Leftrightarrow y \notin y$. The axiom schema of comprehension avoids this by insisting that we can only use a formula φ to cut sets out of pre-existing sets, not to create a set out of thin air.

Note that Comprehension gives us the empty set, if we take (say) $\varphi(z) = z \neq z$.

6. Infinity.
$$\exists x.\emptyset \in x \wedge \forall y.(y \in x \Rightarrow (y \cup \{y\}) \in x).$$
The set asserted to exist by this axiom looks like
$$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots\}$$
and is called ω.

Note that axioms 1–5 are all true in V_ω, the collection of hereditarily finite sets. The axiom of infinity is the only one which requires the existence of transfinite ordinals.

Also, observe that $V_{\omega+\omega}$ models axioms 1-6. These axioms, plus the Axiom of Choice, constituted Zermelo's 1908 theory. Skolem and Frankel added the next axiom to force the existence of a larger universe.

To see the problem, note that in $V_{\omega+\omega}$ we can define the function $n \mapsto \omega + n$, but this is a function whose domain is V_ω but whose range is not a set in $V_{\omega+\omega}$! This seems strange. So, Skolem and Frankel added...

7. Replacement.
$$\begin{aligned}\forall x.\forall y.\forall z.((\varphi(x,y) \wedge \varphi(x,z)) &\Rightarrow z = y) \\ &\Rightarrow \forall w.\exists v.\forall u.(u \in v \Leftrightarrow \exists x.x \in w \wedge \varphi(x,u)).\end{aligned}$$
If φ defines a functional relation, then the image of any set under φ is also a set.

This forces the universe to be much larger: in fact, we can (and will) show that if V_θ models these axioms, then θ is a *strongly inaccessible cardinal*, whose existence cannot be proven within ZFC!

There are still two additional axioms: the Axiom of Foundation (aka Regularity) and the Axiom of Choice; we'll discuss them later.

Lecture 2: Well-orderings
January 21, 2009

3 Well-orderings

Definition 3.1. A *binary relation* r on a set A is a subset of $A \times A$. We also define

$$\begin{aligned} \mathrm{dom}(r) &= \{\, x \mid \exists y.(x,y) \in r \,\}, \\ \mathrm{rng}(r) &= \{\, y \mid \exists x.(x,y) \in r \,\}, \text{and} \\ \mathrm{fld}(r) &= \mathrm{dom}(r) \cup \mathrm{rng}(r). \end{aligned}$$

Definition 3.2. A binary relation r is a *strict partial order* iff

- $\forall x.(x,x) \notin r$, and
- $\forall xyz.$ if $(x,y) \in r$ and $(y,z) \in r$ then $(x,z) \in r$,

that is, if r is irreflexive and transitive. Moreover, iff for all x and y in $\mathrm{fld}(r)$, either $(x,y) \in r$ or $(y,x) \in r$ or $x = y$, we say r is a *strict linear order*.

Definition 3.3. A strict linear order r is a *well-ordering* iff every non-empty $z \subseteq \mathrm{fld}(r)$ has an r-least member.

Remark. For example, the natural numbers $\mathbb{N}$ are well-ordered under the normal $<$ relation. However, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{Q}^+$ are not.

However, we want to be able to talk about well-orderings longer than ω. For example,

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

is an alternative well-ordering of the natural numbers which is longer than ω.

Definition 3.4. $f : X \to X$ is *order-preserving* iff for all $y, z \in X$, $y < z$ implies that $f(y) < f(z)$.

Theorem 3.5. *If $\langle X, < \rangle$ is a well-ordering and f is order-preserving, then for every $y \in X$, $y \leq f(y)$.*

Proof. Suppose otherwise, namely, that there exists some $z \in X$ for which $f(z) < z$. Let z_0 be the least such z. Since f is order preserving, we we also have that $f(f(z_0)) < f(z_0)$; but this contradicts the minimality of z_0. ∎

Remark. One formulation of the Axiom of Choice states that for every set x, there exists some binary relation r such that $\langle x, r \rangle$ is a well-ordering.

Theorem 3.6. *If $<$ well-orders x, then the only automorphism of $\langle x, < \rangle$ is the identity. Such a structure is called* rigid.

Proof. Let f be an automorphism (that is, an order-preserving, onto map) of $\langle x, < \rangle$. (Note that if f is order-preserving, it must be 1-1 as well.) We first note that f^{-1} is also order-preserving: if $y < z$ but $f^{-1}(y) \geq f^{-1}(z)$, we could apply f to both sides to derive a contradiction. Therefore, by Theorem 3.5, for any $y \in x$, we have $f(y) \geq y$ and $f^{-1}(y) \geq y$. Applying f to both sides of the latter inequality, we obtain $y \geq f(y)$; hence $y = f(y)$ and f is necessarily the identity. ∎

Corollary 3.7. *If $\langle x, < \rangle$ and $\langle y, <' \rangle$ are isomorphic well-orderings, there is a unique isomorphism between them. Otherwise, we could derive a non-trivial automorphism by composing one isomorphism with the inverse of another.*

Definition 3.8. Given $\langle x, < \rangle$ and $y \in x$, we can define the *initial segment of x determined by y*,

$$\mathrm{Init}(x, y, <) = \{\, z \in x \mid z < y \,\}.$$

Theorem 3.9. *If $\langle x, < \rangle$ is a well-ordering, there is no $z \in x$ for which $\langle x, < \rangle$ is isomorphic to* $\mathrm{Init}(x, z, <)$.

Remark. This is certainly *not* true for non-well-orderings. For example, $\langle \mathbb{Q}, < \rangle \cong \mathrm{Init}(\mathbb{Q}, z, <)$ for every $z \in \mathbb{Q}$!

Proof. Suppose $z \in x$ such that $\langle x, < \rangle \cong \mathrm{Init}(x, z, <)$. This is an order-preserving map that sends z to something less than itself; this contradicts Theorem 3.5. ∎

Theorem 3.10. *For every pair of well-orderings $w = \langle x, < \rangle$ and $w' = \langle y, <' \rangle$, either*

- $w \cong w'$,
- $w \cong \mathrm{Init}(w', z, <')$ *for some $z \in y$, or*
- $w' \cong \mathrm{Init}(w, z, <)$ *for some $z \in x$.*

Proof. Consider the set

$$f = \{\, (z, z') \mid z \in x, z' \in y, \mathrm{Init}(x, z, <) \cong \mathrm{Init}(y, z', <') \,\}.$$

We first show that f is a function. If we had (z, z') and (z, z'') both elements of f, with $z' \neq z''$, then we would have $\mathrm{Init}(y, z') \cong \mathrm{Init}(x, z) \cong \mathrm{Init}(y, z'')$. However, one of $\mathrm{Init}(y, z')$ and $\mathrm{Init}(y, z'')$ is an initial segment of the other, so this contradicts Theorem 3.9.

A similar argument shows that f is 1-1.

Note that $\mathrm{dom}(f)$ is an initial segment of $\langle x, < \rangle$, and $\mathrm{rng}(f)$ is an initial segment of $\langle y, <' \rangle$. Also note that either $\mathrm{dom}(f) = x$ or $\mathrm{rng}(f) = y$, since otherwise f could be extended. The three cases stated in the theorem correspond precisely to when both the domain and range of f are full, when the domain is full, and when the range is full. ∎

Lecture 3: Ordinals, transfinite induction
January 26, 2009

4 Ordinals

The ordinals are canonical well-ordered sets.

Definition 4.1. A set x is *transitive* iff $\forall y.y \in x \implies y \subseteq x$.

Remark. If z is transitive, then $x \in y \in z \implies x \in z$.

Definition 4.2. x is an *ordinal* iff

- x is transitive, and
- $\langle x, \in\restriction x\rangle$ is a well-ordering.

Remark. In what follows, we use α, β, and γ to refer to arbitrary ordinals.

Lemma 4.3. *If $x \in \alpha$, then x is an ordinal.*

Proof. Since α is transitive, $x \subseteq a$; therefore it is clear that $\langle x, \in\restriction x\rangle$ is a well-ordering since $\langle \alpha, \in\restriction \alpha\rangle$ is. To see that x is transitive, suppose the contrary. That is, suppose there is some $y \in x$ and $z \in y$ such that $z \notin x$. Note that x, y, and z are all elements of α, since α is transitive. Since α is well-ordered under $\in$, either $x = z$ or $x \in z$. If $x = z$, then $z \in y \in z$, contradicting the fact that α is well-ordered; if $x \in z$, then $x \in z \in y \in x$, contradicting the fact that x is well-ordered. ∎

Lemma 4.4. *If $\beta \subseteq \alpha$ and $\beta \neq \alpha$ then $\beta \in \alpha$.*

Proof. Consider the set $\alpha - \beta$, which is nonempty by the given premises. Let γ be the $\in$-least element of $\alpha - \beta$. Then $\beta = \gamma$, which can be shown as follows.

($\subseteq$). Suppose there is some element $x \in \beta$ for which $x \notin \gamma$. Since x and γ are both elements of α, we must therefore have $\gamma \leq x \in \beta$. Since β is transitive, this implies that $\gamma \in \beta$, a contradiction.

($\supseteq$). Suppose $x \in \gamma$; then we must also have $x \in \beta$, since otherwise it would be an element of $\alpha - \beta$ less than γ, contradicting the definition of γ. ∎

Lemma 4.5. *For every α, β, either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.*

Proof. Suppose otherwise. Consider $\gamma = \alpha \cap \beta$, which by assumption is a proper subset of both α and β. It is easy to check that γ is an ordinal. But then by Lemma 4.4, $\gamma \in \alpha$ and $\gamma \in \beta$, so $\gamma \in \alpha \cap \beta = \gamma$, a contradiction. ∎

Theorem 4.6. *The class of ordinals is well-ordered by $\in$.*

Proof. This follows directly from Lemmas 4.4 and 4.5. ∎

Theorem 4.7. *For every set x there is an α such that $\alpha \notin x$.*

Proof. The proof of this theorem is the *Burali-Forti paradox*. Suppose there is a set x of which every ordinal is an element. Then by comprehension we may form the set

$$ord = \{\, \alpha \in x \mid \alpha \text{ is an ordinal} \,\}.$$

But by Theorem 4.6 we can see that ord is well-ordered; by Lemma 4.3 it is transitive; hence, $ord \in ord$, a contradiction. ∎

Remark. Theorem 4.7 can equivalently be stated as "the class of ordinals is a proper class."

Some examples of ordinals:

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

can all easily be checked to be ordinals. Also, if α is an ordinal, then $\alpha \cup \{\alpha\}$ is also.

Definition 4.8. The *successor* of α, denoted $\alpha + 1$, is $\alpha \cup \{\alpha\}$.

Theorem 4.9. *$\alpha + 1$ is an ordinal. Moreover, it is the least ordinal bigger than α.*

Proof. It is easy to see that $(\alpha \cup \{\alpha\}, \in)$ is a strict linear order: for any $x, y \in \alpha \cup \{\alpha\}$, with $x \neq y$, either $x, y \in \alpha$ (in which case $x \in y$ or $y \in x$), or one of x, y is equal to α and the other is an element of α. That every non-empty subset has an $\in$-least member follows easily. To see that $\alpha \cup \{\alpha\}$ is transitive, it suffices to note that $\alpha \subseteq \alpha \cup \{\alpha\}$.

To show that $\alpha + 1$ is the least ordinal bigger than α, suppose that $\beta > \alpha$. Then by definition, $\alpha \in \beta$, and therefore $\alpha \subseteq \beta$; so $\alpha + 1 = \alpha \cup \{\alpha\} \subseteq \beta$. By Lemma 4.4, $\alpha + 1 \leq \beta$. ∎

Definition 4.10. α is a *successor ordinal* iff $\alpha = \beta + 1$ for some β. Otherwise, α is a *limit ordinal*.

Definition 4.11. The smallest non-zero limit ordinal is called ω (and it exists by the Axiom of Infinity). The elements of ω are called *natural numbers*.

Definition 4.12. $x \sim y$ iff there exists a functional relation which is a 1-1, onto mapping from x to y.

Definition 4.13. A set x is *finite* iff there exists some $n \in \omega$ for which $x \sim n$.

Theorem 4.14. *For every well-ordering $\langle x, < \rangle$ there is an ordinal α such that $\langle x, < \rangle$ is isomorphic to $\langle \alpha, \in \restriction \alpha \rangle$.*

Proof. XXX finish me! ∎

Theorem 4.15 (Transfinite Induction)**.** *If*

1. $\varphi(\emptyset)$,
2. $\varphi(\alpha) \implies \varphi(\alpha + 1)$, *and*
3. $\lim(\lambda) \wedge (\forall \beta . \beta < \lambda \implies \varphi(\beta)) \implies \varphi(\lambda)$,

then $\forall \beta . \varphi(\beta)$.

Proof. Suppose not; let γ be the $\in$-minimal ordinal for which $\neg\varphi(\gamma)$. A simple argument by cases (whether γ is $\emptyset$, a successor ordinal, or a limit ordinal) shows that γ cannot exist. ☒

Lecture 4: Transfinite recursion, cardinals
January 28, 2009

Definition 4.16. The class of *sequences Seq* is defined by

$$Seq = \{ f \mid \mathrm{ord}(\mathrm{dom}(f)) \wedge f \text{ is a function} \}.$$

Theorem 4.17 (Transfinite Recursion)**.** *For any functional relation $G : Seq \to V$, there exists a unique functional relation F satisfying*

$$F(\alpha) = G(F \restriction \alpha)$$

for all α.

Proof. We will show that for every α there is a unique function f_α such that $\mathrm{dom}(f_\alpha) = \alpha$, and $\forall \beta < \alpha$,

$$f_\alpha(\beta) = G(f_\alpha \restriction \beta),$$

and $\forall \gamma < \beta$, $f_\beta \restriction \gamma = f_\gamma$.

The proof is by transfinite induction.

- $\alpha = 0$. $f_\alpha = \{\}$ trivially satisfies the conditions.
- $\alpha = \beta + 1$. By the IH, assume there exists a unique f_β that satisfies the conditions. Now let

$$f_{\beta+1}(\gamma) = \begin{cases} f_\beta(\gamma) & \gamma < \beta \\ G(f_\beta) & \gamma = \beta. \end{cases}$$

  We must show that for every $\delta < \beta + 1$, $f_{\beta+1}(\delta) = G(f_{\beta+1} \restriction \delta)$. There are two cases.

  - If $\delta = \beta$, then $f_{\beta+1}(\delta) = G(f_\beta) = G(f_{\beta+1} \restriction \beta)$, since it is clear from the definition of $f_{\beta+1}$ that $f_{\beta+1} \restriction \beta = f_\beta$.
  - If $\delta < \beta$, then $f_{\beta+1}(\delta) = f_\beta(\delta)$, which is equal to $G(f_\beta \restriction \delta)$ by the IH. But this is equal to $G(f_{\beta+1} \restriction \delta)$ by definition of $f_{\beta+1}$.

  By the IH, we already know that $f_\beta \restriction \zeta = f_\zeta$ for all $\zeta < \beta$; we must show that forall $\zeta < \beta + 1$, $f_{\beta+1} \restriction \zeta = f_\zeta$. First, if $\zeta < \beta$, this follows from the IH and the definition of $f_{\beta+1}$. If $\zeta = \beta$, we must show $f_{\beta+1} \restriction \beta = f_\beta$; this follows immediately from the definition of $f_{\beta+1}$.

  The last thing we must show is that $f_{\beta+1}$ is unique. Suppose there is some h which also satisfies the conditions, that is, $\mathrm{dom}(h) = \beta + 1$ and $\forall \delta < \beta + 1, h(\delta) = G(h \restriction \delta)$. Then pick $\delta < \beta + 1$ to be the smallest ordinal for which $h(\delta) \neq f_{\beta+1}(\delta)$. Then $f_{\beta+1} \restriction \delta = h \restriction \delta$, so $f_{\beta+1}(\delta) = G(f_{\beta+1} \restriction \delta) = G(h \restriction \delta) = h(\delta)$, a contradiction.

- $\lim(\alpha)$. By the IH, assume that for all $\beta < \alpha$, there exists a f_β satisfying the conditions. Then let $f_\alpha = \bigcup_{\beta<\alpha} f_\beta$.

  First, we must show that f_α is a set. This follows from the Axiom of Replacement, since it is the union of the image of α under the map $\beta \mapsto f_\beta$, which is a functional relation by the uniqueness of f_β under the IH.

  The fact that f_α is functional follows from the IH, since we know that $f_\beta \restriction \gamma = f_\gamma$ for all $\gamma < \beta$.

  Let $\beta < \alpha$. Then

  $$\begin{aligned} f_\alpha(\beta) &= f_{\beta+1}(\beta) && \beta + 1 < \alpha, \text{ def. of } f_\alpha \\ &= G(f_{\beta+1} \restriction \beta) && \text{IH} \\ &= G(f_\alpha \restriction \beta) && \text{intuitively obvious...?} \end{aligned}$$

  We need do nothing to establish that $\forall \gamma < \beta < \alpha$, $f_\beta \restriction \gamma = f_\gamma$; it already holds by the inductive hypothesis.

  The argument for the uniqueness of f_α is the same as in the previous case.

Now define $F(\alpha) = G(f_\alpha)$. We claim that F satisfies the theorem. Note that F is a functional relation since we have defined it pointwise. Note also that $F \restriction \alpha$ is a set (by Replacement: $F \restriction \alpha = \{(\beta, F(\beta)) \mid \beta \in \alpha\}$). To see that $f_\alpha = F \restriction \alpha$, consider any $\beta \in \mathrm{dom}(f_\alpha) = \mathrm{dom}(F \restriction \alpha) = \alpha$; we have $f_\alpha(\beta) = G(f_\alpha \restriction \beta) = G(f_\beta) = F(\beta)$. ∎

5 Cardinals

Definition 5.1. X is *equivalent* to Y, denoted $X \sim Y$ (or $|X| = |Y|$), if there is a mapping $f : X \xrightarrow[\text{onto}]{\text{1-1}} Y$.

Definition 5.2. $X \leq Y$ if there is a mapping $f : X \xrightarrow{\text{1-1}} Y$.

Theorem 5.3 (Cantor-Schröder-Bernstein)**.** $X \leq Y \wedge Y \leq X \implies X \sim Y$.

Proof. Suppose $f : X \xrightarrow{\text{1-1}} Y$ and $g : Y \xrightarrow{\text{1-1}} X$ are functions implied by the premises. Let

$$\begin{aligned} X_0 &= X - g(Y) \\ X_{n+1} &= (g \circ f)(X_n) \\ X_\omega &= \bigcup_{n\in\omega} X_n. \end{aligned}$$

and define

$$h(a) = \begin{cases} f(a) & a \in X_\omega \\ g^{-1}(a) & a \in X - X_\omega. \end{cases}$$

Note that h is total, since if $a \in X - X_\omega$, then $a \notin X_0$, so $a \in \text{rng}(g)$ and $g^{-1}(a)$ is defined.

We claim that h is a one-to-one, onto function from X to Y.

- To show that h is one-to-one, suppose $a, b \in X$ and $h(a) = h(b)$. If $a, b \in X_\omega$, then $f(a) = f(b)$, so $a = b$ since f is one-to-one. If $a, b \notin X_\omega$, then $g^{-1}(a) = g^{-1}(b)$; applying g to both sides yields $a = b$. So, without loss of generality, suppose $a \in X_\omega$ and $b \notin X_\omega$, $f(a) = g^{-1}(b)$; we claim this case is impossible. Applying g to both sides yields $g(f(a)) = b$; but since $a \in X_\omega$ then b is also, a contradiction.

- Now we show h is onto. Let $b \in Y$, and let $f(X_\omega) = Y_\omega$. If $b \in Y_\omega$, then it is in the image of h, since $h(X_\omega) = f(X_\omega) = Y_\omega$. Otherwise, consider $g(b)$. $g(b) \notin X_\omega$; if it were, $g(b) \in X_n$ for some n, so we would have $g(b) = g(f(q))$ for some $q \in X_{n-1}$. But since g is one-to-one, this implies $b = f(q)$, that is, $b \in Y_\omega$, a contradiction. Therefore, $h(g(b)) = g^{-1}(g(b)) = b$.

SDG

Definition 5.4. $X < Y$ if $X \leq Y$ and $Y \not\leq X$.

Theorem 5.5 (Cantor diagonal)**.** *For every X, there exists a Y such that $X < Y$.*

Proof. Claim: $X < \mathcal{P}(X)$. Let $f : X \to \mathcal{P}(X)$, and define

$$a = \{\, b \in X \mid b \notin f(b) \,\}.$$

Note that $a \in \mathcal{P}(X)$. We claim that $a \notin \text{rng}(f)$. If it were, there would be some $c \in X$ with $f(c) = a$; is $c \in f(c)$? If it is, it isn't; if it isn't, it is. So there. f is not onto.

Note that $X \leq \mathcal{P}(X)$, since $f(a) = \{a\}$ is a one-to-one mapping.

If $\mathcal{P}(X) \leq X$, by Cantor-Schröder-Bernstein there would be a one-to-one, onto map between them, but we have shown that any mapping $X \to \mathcal{P}(X)$ is not onto. Therefore, $X < \mathcal{P}(X)$. SDG

Remark. Why is this called a *diagonal* argument? Note that $\mathcal{P}(X) \sim 2^X$ (where X^Y, also sometimes written ${}^Y X$, denotes the set of functions from Y to X). In particular, if $Z \subseteq X$, we set $Z \in \mathcal{P}(X)$ to the indicator function

$$g_Z(a) = \begin{cases} 1 & a \in Z \\ 0 & a \notin Z. \end{cases}$$

In the special case that $X \sim \omega$, if we assume there exists a 1-1, onto mapping from X to $\mathcal{P}(X)$, we can make a table of the indicator functions to which each element of X is sent, as follows:

	x_0	x_1	x_2	x_3	$\dots$
x_0	1	0	1	1	
x_1	0	1	0	1	
x_2	0	0	0	1	
x_3	1	0	0	0	
$\vdots$					$\ddots$

The ith row is the indicator function describing the subset to which x_i is sent. Now we simply note that the argument in the above proof corresponds to picking out the diagonal elements (here $1, 1, 0, 0, \dots$), flipping them $(0, 0, 1, 1, \dots)$, and noting that the resulting sequence cannot be a row of the table.

Definition 5.6. κ is a *cardinal* iff κ is an ordinal such that $\alpha \not\sim \kappa$ for all $\alpha \in \kappa$.

Remark. A cardinal κ is an *initial ordinal*—the smallest ordinal having its cardinality.

Exercise: show that every natural number is a cardinal, and that ω is a cardinal (ω is the first infinite cardinal).

Remark. By Theorem 5.5, we know that $\omega < \mathcal{P}(\omega)$. A natural question arises: is there some $X \subseteq \mathcal{P}(\omega)$ for which $\omega < X < \mathcal{P}(\omega)$? This is an interesting question, especially given that it can be shown that $\mathbb{R} \sim \mathcal{P}(\omega)$. Hilbert thought this question so important that he made it the very first problem in his famous 1900 list.

Cantor hypothesized that there does not exist such an X; this hypothesis is known as the *continuum hypothesis* (CH). This is a reasonable hypothesis, especially given the establishment of various special cases, such as the fact that for all $X \subseteq \mathbb{R}$, if X is closed, then it is not the case that $\omega < X < \mathbb{R}$ (Cantor-Bendixson).

It turns out that the continuum hypothesis is independent of ZF: Gödel in 1939 showed that the consistency of ZF implies the consistency of ZF + AC + CH; but Cohen showed in 1963 that the consistency of ZF also implies the consistency of ZF + AC + $\neg$ CH.

Lecture 5: Cardinals
February 2, 2009

Definition 5.7 (Well-ordering principle)**.** For every set X, there exists a bijection $f : \alpha \xrightarrow[\text{onto}]{\text{1-1}} X$ for some ordinal α.

Remark. In other words, the well-ordering principle states that every set X can be well-ordered, since there is a 1-1 projection from some ordinal onto X.

Definition 5.8 (Axiom of Choice)**.** For every set X which is a collection of nonempty sets, there exists a function f with $\text{dom}(f) = X$ and for every $y \in X$, $f(y) \in y$.

Remark. f is a "choice function" which chooses one element of each element of X.

Theorem 5.9. *The well-ordering principle and axiom of choice are equivalent.*

Proof. (WOP $\implies$ AC) Suppose X is a collection of nonempty sets. Then let $Z = \bigcup X$. By the well-ordering principle, there is some ordinal δ and some function g for which

$$Z = \{\, g(\gamma) \mid \gamma < \delta \,\}.$$

But then let $f : X \to Z$ be defined by $f(y) = g(\beta)$ where β is the least ordinal for which $g(\beta) \in y$. By definition, $\text{dom}(f) = X$ and $f(y) \in y$ for every $y \in X$. To see that f is well-defined, just note that $y \subseteq Z$ and g is onto.

(AC $\implies$ WOP) Let X be a set and define

$$Z = \mathcal{P}(X) - \{\emptyset\},$$

which is clearly a collection of nonempty sets. Let f be a choice function for Z. Then define

$$G(\beta) = f\big(X - \{\, G(\gamma) \mid \gamma < \beta \,\}\big),$$

which is clearly 1-1. Then for some δ, we have $\{\, G(\beta) \mid \beta < \delta \,\} = X$; otherwise, G would be a 1-1 function from the ordinals into X, and the ordinals would be a set (by the Replacement Axiom under G^{-1} applied to X), a contradiction.

Therefore $G \restriction \delta$ is a bijection from δ to X. ∎

Definition 5.10. The *cardinality* of X, denoted $|X|$, is the least β for which there exists an $f : \beta \xrightarrow[\text{onto}]{\text{1-1}} X$.

Remark. It is easy to see that the cardinality of any set is a cardinal (the proof is left as an exercise for the reader).

Note that we require the Axiom of Choice/Well Ordering Principle for the cardinality operator $|-|$ to be well-defined.

Theorem 5.11. *For every cardinal κ, there exists a cardinal λ with $\kappa < \lambda$.*

Proof. This follows from Cantor's theorem, since $\kappa < 2^\kappa$. ∎

Corollary 5.12. *It follows that the class of cardinals is a proper class. For if there were a set X of all cardinals, then $\bigcup X = Ord$ would be a set.*

Remark. The proof of Theorem 5.11 implicitly relied on the Axiom of Choice in its use of cardinality. We can also supply an alternative proof that does not use the Axiom of Choice:

Proof. Let κ be a cardinal and consider an ordinal $\lambda > \kappa$. If there is a 1-1 map from λ to κ, it defines a well-ordering on a subset of κ. However, the class of well-orderings on subsets of κ form a set: a well-ordering on any particular subset $z \in \mathcal{P}(\kappa)$ is just an element of the set $\mathcal{P}(z \times z)$, so by the axioms of replacement and restriction we may form the set of all such well-orderings.

Therefore, there cannot exist a 1-1 map from *every* ordinal larger than κ into κ; otherwise the ordinals would form a set.

So, choose the least ordinal for which there does not exist a 1-1 map into κ; this is the next cardinal after κ, denoted κ^+. ∎

Definition 5.13. By transfinite recursion, we define

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

Remark. We note that $\aleph_\lambda$ is a cardinal: suppose there is some $f : \aleph_\lambda \xrightarrow{1\text{-}1} \gamma$, for some $\gamma < \aleph_\lambda$. Then for some $\beta < \lambda$, $\gamma < \aleph_\beta$. But then $f \restriction \aleph_{\beta+1}$ is a 1-1 function from $\aleph_{\beta+1}$ into a subset of $\aleph_\beta$, which is a contradiction by defition of $\aleph_{\beta+1}$.

Definition 5.14. $f : Ord \to Ord$ is a *normal function* iff f is order-preserving and continuous at limits (that is, $f(\lambda) = \sup_{\beta<\lambda}(f(\beta))$ for λ a limit ordinal).

Theorem 5.15. *Every normal function has arbitrarily large fixed points.*

Proof. Let f be a normal function, and pick any α. Define

$$\begin{aligned} \beta_0 &= \alpha \\ \beta_{n+1} &= f(\beta_n) \\ \beta &= \sup_{n\in\omega} \beta_n. \end{aligned}$$

Note that since f is order-preserving, $\beta_0 \leq \beta_1$. Then we have

$$\begin{aligned} f(\beta) &= \sup_{n\in\omega}(f(\beta_n)) && f \text{ is continuous} \\ &= \sup_{n\in\omega}\{\beta_{n+1}\} && \text{defn. of } \beta \\ &= \sup_{n\in\omega}\{\beta_n\} && \beta_0 \leq \beta_1 \\ &= \beta && \text{defn. of } \beta \end{aligned}$$

Hence β is a fixed point of f which is at least α. ∎

Remark. Note that $\aleph_{(-)}$ is a normal function; hence, there are arbitrarily large ordinals γ with $\gamma = \aleph_\gamma$!

Definition 5.16 (Cofinality)**.**

- $X \subseteq \alpha$ is *cofinal in* α iff $\sup(X) = \alpha$.
- A map $f : \beta \to \alpha$ is a *cofinal map* iff $\operatorname{rng} f$ is cofinal in α.
- The *cofinality of* α, denoted $\operatorname{cf}(\alpha)$, is the least β for which there exists a cofinal map $f : \beta \to \alpha$.

Remark. For example, $\operatorname{cf}(\omega) = \operatorname{cf}(\omega + \omega) = \operatorname{cf}(\aleph_\omega) = \omega$.

Note that all the fixed points constructible by the method in the proof of Theorem 5.15 have cofinality ω. This begs the question of whether there exist fixpoints with greater cofinality.

Exercise: show that if $\alpha > 0$ is a limit ordinal, then $\operatorname{cf}(\alpha)$ is a cardinal.

From now on when discussion cofinality we assume that any ordinals mentioned are nonzero limit ordinals. κ and λ will conventionally refer to cardinals.

Definition 5.17.

- κ is *regular* iff $\operatorname{cf}(\kappa) = \kappa$; otherwise it is *singular*.
- κ is a *limit cardinal* iff $\lambda < \kappa \implies \lambda^+ < \kappa$.
- κ is a *strong limit cardinal* iff $\lambda < \kappa \implies 2^\lambda < \kappa$.
- κ is *weakly inaccessible* iff it is a regular limit cardinal.
- κ is *(strongly) inaccessible* iff it is a regular strong limit cardinal,

Remark. To look ahead, we will show that if θ is strongly inaccessible, then $\langle V_\theta, \epsilon \restriction V_\theta \rangle \models \text{ZFC}$.

The SI axiom asserts that there exists a strongly inaccessible cardinal; this axiom cannot be derived in ZFC.

Definition 5.18 (Cardinal arithmetic)**.**

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

Theorem 5.19 (Cardinal arithmetic is trivial)**.** *For all* $\kappa, \lambda \geq \omega$, $\kappa \times \lambda = \kappa + \lambda = \max(\kappa, \lambda)$.

Proof. We begin by defining a canonical map $\Gamma : Ord \times Ord \to Ord$. In particular, define $(\alpha, \beta) \prec (\gamma, \delta)$ iff either $\max(\alpha, \beta) < \max(\gamma, \delta)$, or the max's are equal and (α, β) is lexicographically smaller than (γ, δ). This defines a well-ordering on $Ord \times Ord$. Then we can define

$$\Gamma(\alpha, \beta) = \delta, \qquad \langle \delta, \epsilon \rangle \simeq \operatorname{Init}(Ord \times Ord, (\alpha, \beta), \prec).$$

We claim that $\Gamma[\kappa \times \kappa] = \kappa$ for every infinite κ, which we show by transfinite induction.

For the base case, we note that $\Gamma[\omega \times \omega] = \omega$, which is left as an exercise for the reader.

In the inductive case, let κ be the least cardinal greater than ω such that $\Gamma[\kappa \times \kappa] \neq \kappa$. Then for some $\alpha, \beta \in \kappa$, $\Gamma(\alpha, \beta) = \kappa$. Choose δ so $\max(\alpha, \beta) < \delta < \kappa$. Now, (δ, δ) determines an initial segment of $Ord \times Ord$ which contains (α, β), so $\Gamma[\delta \times \delta] \supset \kappa$, and hence $|\delta \times \delta| \geq \kappa$. However, by minimality of κ, $|\delta * \delta| = |\delta| \cdot |\delta| = |\delta| < \kappa$, a contradiction. ∎

Lecture 6: Regularity, CH, and König's Theorem
February 4, 2009

Lemma 5.20. *Suppose that X is a collection of sets, and that $|X| = \kappa$ and $\sup\{\, |Z| \mid Z \in X \,\} = \lambda$. Then $|\bigcup X| \leq \kappa \times \lambda$.*

Proof. By the well-ordering principle (AC), we can make an enumeration of X,

$$X = \{\, Z_\alpha \mid \alpha < \kappa \,\}.$$

For each α, $|Z_\alpha| = \lambda_\alpha < \lambda$. Again by the well-ordering principle, we can make an enumeration of each Z_α,

$$Z_\alpha = \{\, u_{\alpha\beta} \mid \beta < \lambda_\alpha \}.$$

Then we can write $\bigcup X$ as

$$\bigcup X = \{\, u_{\alpha\beta} \mid \alpha < \kappa,\, \beta < \lambda_\alpha \,\},$$

which clearly has cardinality at most $\kappa \times \lambda$. ∎

Remark. This result is in some sense a generalization of the fact that $\mathbb{Q}$ is countable, with one important difference. To show that the rationals are countable, we just have to exhibit a bijection between the rationals (or, more simply, between $\mathbb{N} \times \mathbb{N}$) and the naturals. From this result, it seems like it should follow that if X is a countable collection of countable sets, then $\bigcup X$ is also countable; but to show this, we need the AC (which we don't need to show the countability of $\mathbb{Q}$). Intuitively, this is because we need to be able to "pick" an ordering for each $Z \in X$.

The above result is more general yet: instead of talking about a countable union of countable sets, is about a cardinality-κ union of sets with cardinality at most λ; the fact about countable sets in particular follows from the fact that $\omega \times \omega = \omega$.

Lemma 5.21. *For every ordinal α, there exists a strictly increasing cofinal map from $\mathrm{cf}(\alpha)$ to α.*

Proof. Let $g : \mathrm{cf}(\alpha) \to \alpha$ be a cofinal map. Then define $f : \mathrm{cf}(\alpha) \to \alpha$ by

$$f(\beta) = \max\{g(\beta), \sup_{\gamma<\beta}(f(\gamma) + 1)\}.$$

By definition, $\sup(\mathrm{rng}(f)) \geq \sup(\mathrm{rng}(g)) = \alpha$, so f is cofinal. f is also strictly increasing: if $\beta > \gamma$, then $f(\beta) > \sup_{\gamma<\beta} f(\gamma) \geq f(\gamma)$. ∎

Lemma 5.22. cf *is idempotent.*

Proof. Let α, β, and γ be ordinals such that $\mathrm{cf}(\alpha) = \beta$ and $\mathrm{cf}(\beta) = \gamma$. By Lemma 5.21, suppose $f : \beta \to \alpha$ and $g : \gamma \to \beta$ are strictly increasing cofinal maps. Let $\delta \in \alpha$. Since f is a cofinal map into α, there must be some $\zeta \in \beta$ for which $f(\zeta) > \delta$. Likewise, there must be some $\eta \in \gamma$ for which $g(\eta) > \zeta$. Since f is strictly increasing, we conclude that $f(g(\eta)) > f(\zeta) > \delta$; hence $f \circ g$ is a cofinal map into α, and $\beta = \gamma$. ∎

Lemma 5.23. *If $\alpha > 0$ is a limit ordinal, then $\mathrm{cf}(\alpha)$ is an infinite, regular cardinal.*

Proof. By definition, $\mathrm{cf}(\alpha)$ is the least β for which there exists a cofinal map $f : \beta \to \alpha$ (that is, for which $\sup(\mathrm{rng}(f)) = \alpha$). Suppose that $\mathrm{cf}(\alpha)$ is not a cardinal. Then there exists some $\gamma < \mathrm{cf}(\alpha)$ such that $\gamma \sim \mathrm{cf}(\alpha)$, that is, there exists some $g : \gamma \xrightarrow[\text{onto}]{\text{1-1}} \mathrm{cf}(\alpha)$. But then $f \circ g : \gamma \to \alpha$ is also a cofinal map, contradicting the minimality of $\mathrm{cf}(\alpha)$. Also, $\mathrm{cf}(\alpha)$ must be infinite since there cannot exist a cofinal map from a finite set into an infinite one; $\mathrm{cf}(\alpha)$ is regular by Lemma 5.22. ∎

Theorem 5.24. *For every $\kappa \geq \omega$, κ^+ is regular. That is, $\aleph_{\alpha+1}$ is regular for all α.*

Remark. To help provide some intuition for the relationship of this theorem to Lemma 5.20, we can show the following special case, namely, that $\omega^+ = \aleph_1$ is regular.

Suppose otherwise, namely, that $\mathrm{cf}(\aleph_1) = \omega$ (note, by Lemma 5.23, that this is the only choice for $\mathrm{cf}(\aleph_1)$ if $\aleph_1$ is not regular). That is, for some $f : \omega \to \aleph_1$, $\mathrm{rng}(f)$ is cofinal in $\aleph_1$, *i.e.*, $\bigcup \mathrm{rng}(f) = \aleph_1$. Now, we note the following facts:

- $|\mathrm{rng}(f)| = \omega$. This is clear since $\mathrm{dom}(f) = \omega$.
- For every $\alpha \in \mathrm{rng}(f)$, $|\alpha| \leq \omega$. This follows since $\alpha \in \aleph_1$, so the biggest its cardinality could possibly be is $\aleph_0 = \omega$.

Hence $\bigcup \mathrm{rng}(f)$ is a countable union of countable sets—but we know this is countable, so it cannot be equal to $\aleph_1$.

Proof. We now give a general proof of Theorem 5.24; it follows much the same shape as the preceding remark.

For purposes of contradiction, suppose that $\aleph_{\alpha+1}$ is not regular, that is, there is some cofinal map $f : \aleph_\beta \to \aleph_{\alpha+1}$ where $\beta \leq \alpha$. Then $\bigcup \mathrm{rng}(f) = \aleph_{\alpha+1}$. If $\gamma \in \mathrm{rng}(f)$, then $|\gamma| < \aleph_{\alpha+1}$. Therefore, $|\mathrm{rng}(f)| = \aleph_\beta$ and $\sup(\mathrm{rng}(f)) = \aleph_\alpha$, so by Lemma 5.20, the cardinality of $\bigcup \mathrm{rng}(f)$ is $\alpha \times \beta = \max(\alpha, \beta) < \alpha + 1$, contradicting the cofinality of f. ∎

Remark. Theorem 5.24 asserts that all successor cardinals are regular. However, it turns out that we can't even prove that there *exist* any regular limit cardinals (*i.e.*, weakly inaccessible cardinals) other than ω!

Recall that the Continuum Hypothesis posits that there is no cardinal intermediate between ω and $|\mathcal{P}(\omega)|$; that is, there does not exist a set X such that $\omega < |X| < |\mathcal{P}(\omega)|$. Given the AC, we can reformulate this as the equality

$$2^{\aleph_0} = \aleph_1,$$

that is, $|\mathcal{P}(\omega)|$ is the next cardinal after $\aleph_0$.

This suggests what is known as the Generalized Continuum Hypothesis (GCH):

$$\forall \kappa, 2^\kappa = \kappa^+.$$

Note that in the presence of the GCH, "weakly inaccessible" and "strongly inaccessible" are equivalent.

Using the model of constructible sets, Gödel in 1939 showed that ZF + AC + GCH is consistent if ZF is; it's relatively clear what this system would look like. However, Cohen showed that ZFC + ¬CH is consistent if ZF is; what does ZFC look like with ¬CH? In fact, it turns out that for every $\alpha \geq 0$, ZFC + $(2^{\aleph_0} = \aleph_{\alpha+1})$ is consistent if ZF is! Moreover, for every λ, if $\mathrm{cf}(\lambda) > \omega$, then ZFC + $(2^{\aleph_0} = \aleph_\lambda)$ is consistent if ZF is. That is, $2^{\aleph_0}$ could be $\aleph_1$, or $\aleph_2$, or $\aleph_{\omega+1}$, but it could *not* be $\aleph_\omega$ or $\aleph_{\omega+\omega}$, and so on.

Let's prove that $\mathrm{cf}(2^{\aleph_0}) > \omega$. Strangely enough, in light of the previous remarks, this is just about all we can say about $2^{\aleph_0}$! This will follow as a corollary to Theorem 5.27.

Definition 5.25. Given a collection of sets X_i indexed by the elements of some set I, we may form the sum

$$\sum_{i \in I} X_i = \bigcup_{i \in I} (X_i \times \{i\}),$$

that is, the disjoint union of all the X_i's, using the indices as tags.

Definition 5.26. Given a collection of sets X_i, we may also form the product

$$\prod_{i \in I} X_i = \{\, f : I \to \bigcup_{i \in I} X_i \mid \forall i \in I,\ f(i) \in X_i \,\}.$$

That is, $\prod_i X_i$ is the set of functions which pick out an element of X_i for each $i \in I$. As an example, $\mathbb{R}^3 = \prod_{i \in \{0,1,2\}} \mathbb{R}$ is the set of functions that pick out a real number for each of the three indices 0, 1, and 2; these can also be thought of as ordered triples (although they are not actually triples in a technical sense).

Theorem 5.27 (König, 1905)**.** *Suppose that* $\forall i \in I$, $\kappa_i < \lambda_i$. *Then*

$$\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i.$$

Remark. We defer the proof of Theorem 5.27 to examine two corollaries.

Corollary 5.28 (Cantor's Theorem (Theorem 5.5))**.**

Proof. Let $\kappa_i = 1$ and $\lambda_i = 2$. Then $\sum_{i\in I} 1 \sim I$, and $\prod_{i\in I} 2 \sim \mathcal{P}(I)$. ∎

Corollary 5.29. $\mathrm{cf}(2^{\aleph_0}) > \omega$.

Proof. Let $f : \omega \to 2^{\aleph_0}$, and for $i \in \omega$ let $\kappa_i = |f(i)|$; thus $\kappa_i < 2^{\aleph_0}$. Also, let $\lambda_i = 2^{\aleph_0}$, for all i. Then

$$\sup_{i\in\omega} \kappa_i \leq \sum_{i\in\omega} \kappa_i < \prod_{i\in\omega} \lambda_i = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0\times\aleph_0} = 2^{\aleph_0}.$$ ∎

Proof. We now prove Theorem 5.27. Suppose we have a family of sets Z_i, and let $\lambda_i = |Z_i|$ and $\kappa_i < \lambda_i$ for $i \in I$. Now let $Z = \prod_{i\in I} Z_i$, and for each $i \in I$ pick (by the AC) some $Y_i \subset Z$ with $|Y_i| = \kappa_i$. Then we will show that $\bigcup_{i\in I} Y_i \neq Z$, from which the theorem follows immediately.

For each $i \in I$, define $w_i = \{\, g(i) \mid g \in Y_i \,\}$. Clearly $|w_i| \leq \kappa_i < \lambda_i$. Therefore, $V_i = Z_i - w_i \neq \emptyset$, and $\prod_{i\in I} V_i \neq \emptyset$. (We note in passing that this is another formulation of the AC—that the product of a nonempty collection of nonempty sets is nonempty.)

But $\prod_{i\in I} V_i \subseteq Z$ is disjoint from $\bigcup_{i\in I} Y_i$; hence $\bigcup_{i\in I} Y_i \neq Z$. ∎

Remark. This is a generalized "diagonal" argument, which explains why Cantor's Theorem follows so readily as a corollary. Some additional commentary should go here.

Lecture 7: The Real Line
February 9, 2009

6 The Real Line

Definition 6.1. Let $(\mathbb{Q}, <)$ denote the rational numbers with the usual ordering. We define δ to be a formula of first-order logic which expresses the fact that $\mathbb{Q}$ is a dense linear order without endpoints. (Actually translating this into first-order logic is left as an exercise for the reader.)

Definition 6.2. A *partial isomorphism* of orders is a map which is an isomorphism of its domain and range. That is, $f : C \to D$ is a partial isomorphism if for every $e, e' \in C$, $e \leq_C e' \implies f(e) \leq_D f(e')$ whenever $e, e' \in \mathrm{dom}(f)$.

Definition 6.3. A set P of maps from C to D has the *back-and-forth property* iff

- For every $f \in P$ and $c \in C$, there is some $g \in P$ such that $f \subseteq g$ and $c \in \mathrm{dom}(g)$. (This is the "forth" part.)
- For every $f \in P$ and $d \in D$, there is some $g \in P$ such that $f \subseteq g$ and $d \in \mathrm{rng}(g)$. (You guessed it, the "back" part.)

Definition 6.4. C and D are *partially isomorphic*, denoted $C \cong_P D$ iff there is a nonempty set P of partial isomorphisms between C and D which has the back-and-forth property.

Remark. Note that the existence of a partial isomorphism between C and D does *not*, by itself, imply that C and D are partially isomorphic.

Lemma 6.5. *If $C, D \models \delta$, then $C \cong_P D$.*

Proof. Define P to be the set of order-preserving maps f for which $\mathrm{dom}(f)$ is finite, $\mathrm{dom}(f) \subseteq C$, and $\mathrm{rng}(f) \subseteq D$.

P is nonempty, because any singleton map from some element $c \in C$ to any element $d \in D$ is trivially order-preserving.

To see that P has the "forth" property, suppose $f \in P$ and $c \in C - \mathrm{dom}(f)$. Now suppose $c < \min(\mathrm{dom}(f))$, which exists since $\mathrm{dom}(f)$ is finite. Then, since D has no endpoints, there exists some $d \in D$ for which $d < f(\min(\mathrm{dom}(f)))$. Take $g = f \cup (c, d)$; g is order-preserving so $g \in P$. The case when $c > \max(\mathrm{dom}(f))$ is similar. Otherwise, let c_1 be the greatest element of $\mathrm{dom}(f)$ less than c, and c_2 the least element of $\mathrm{dom}(f)$ greater than c; since D is dense, there is some $d \in D$ for which $f(c_1) < d < f(c_2)$. Again, take $g = f \cup (c, d)$; then $g \in P$.

The proof that P has the "back" property is similar, and uses the fact that $C \models \delta$. ∎

Remark. We note that there are partially isomorphic orders which are not isomorphic—in particular, by the previous lemma, $\mathbb{Q} \cong_P \mathbb{R}$, but we know $\mathbb{Q} \ncong \mathbb{R}$, since they have different cardinality.

Theorem 6.6 (Cantor's back-and-forth theorem)**.** *If the orders C and D are partially isomorphic and* $\mathrm{card}(C) = \mathrm{card}(D) = \aleph_0$*, then $C \cong D$.*

Remark. By saying C is an order, we mean it is a pair $\langle X, <_C \rangle$, and define $\mathrm{card}(C) = \mathrm{card}(X)$.

Proof. Let P be the set of partial isomorphisms witnessing the fact that C and D are partially isomorphic. Since C and D are countable, we may enumerate them as

$$C = \{c_0, c_1, c_2, \dots\}$$
$$D = \{d_0, d_1, d_2, \dots\}.$$

Pick any $f_{-1} \in P$, and enlarge it to f_0 such that $c_0 \in \mathrm{dom}(f_0)$; $f_0 \in P$ since P has the forth property.

Now we choose $f_1, f_2, \dots \in P$ as follows. At stage $2n+1$, pick f_{2n+1} to extend f_{2n} with $d_n \in \mathrm{rng}(f_{2n+1})$; at stage $2n+2$, pick f_{2n+2} to extend f_{2n+1} with $c_n \in \mathrm{dom}(f_{2n+2})$.

Finally, let $f = \bigcup_{i \in \omega} f_i$. f is a function, since $f_0 \subseteq f_1 \subseteq f_2 \subseteq \dots$. Also, $\mathrm{dom}(f) = C$ and $\mathrm{rng}(f) = D$ by construction. Finally, f is order-preserving, since if $c_i <_C c_j$, then $c_i, c_j \in \mathrm{dom}(f_{2\max(i,j)})$, and all the f_k are order-preserving. Therefore, f is an isomorphism. ∎

Corollary 6.7. *For all orders A and B, if* $\mathrm{card}(A) = \mathrm{card}(B) = \aleph_0$ *and $A \models \delta$ and $B \models \delta$, then $A \cong B$.*

Proof. This follows immediately from Lemma 6.5 and Theorem 6.6. ∎

Remark. Note that there are $C, D \models \delta$ where $\mathrm{card}(C) = \mathrm{card}(D) = 2^{\aleph_0}$ but $C \ncong D$. For example, take $C = \mathbb{R}$ and $D = \mathbb{R} - (Irr \cap [0,1])$, where Irr denotes the set of irrational numbers. So δ only categorizes sets of cardinality $\aleph_0$.

Exercise: show that for every $\kappa > \aleph_0$, there are 2^κ pairwise non-isomorphic orders A of cardinality κ ???

Definition 6.8. For a language L, we write $A \equiv_L B$ to mean "A and B can't be distinguished by sentences of L," that is, for all $\varphi \in L$, $A \models \varphi \iff B \models \varphi$.

Remark. $L_{\infty\omega}$ is the maximal language one gets by allowing application of boolean operations ($\bigwedge$, $\bigvee$) to sets of first-order formulas. In other words, $L_{\infty\omega}$ allows infinite conjunction and disjunctions. In general, $L_{\kappa\omega}$ is the language which allows taking the conjunction or disjunction of sets of formulas up to cardinality κ.

Theorem 6.9 (Karp)**.** *If $A \cong_P B$ then $A \equiv_{L_{\infty\omega}} B$.*

Remark. The proof is omitted. We note that this immediately implies that $\mathbb{Q} \equiv_{L_{\infty\omega}} \mathbb{R}$! So we need better tools to distinguish $\mathbb{Q}$ from $\mathbb{R}$. What is true about $\mathbb{R}$ that isn't true about $\mathbb{Q}$?

- $\mathbb{R}$ is *order-complete*; that is, every nonempty bounded set of reals has a least upper bound. This is clearly not true about $\mathbb{Q}$, as noted by the ancient Greeks.
- $\mathbb{R}$ is *seperable*, that is, there exists a countable subset which is dense in $\mathbb{R}$ (for example, $\mathbb{Q}$).

So, let γ denote the sentence whose interpretation is "$\mathbb{R}$ is a complete, separable, dense linear order without endpoints."

We can express γ in second-order logic. In particular, to express the fact that a predicate X corresponds to a countable subset of its domain, we can write

$$\exists S.\text{S is 1-1 and almost onto on } X\text{, and } X, S \text{ satisfies induction.}$$

where "almost onto" means that $|X - \text{rng}(S)| = 1$, and "X, S satisfies induction" means that

$$\forall Y.Y(0) \wedge (Y(n) \wedge S(n,m) \implies Y(m)) \implies (\forall n.X(n) \implies Y(n)).$$

Theorem 6.10. *If $A, B \models \gamma$, then $A \cong B$.*

Proof. Let $\mathbb{Q}^A$ and $\mathbb{Q}^B$ be countable, linearly ordered subsets dense in A and B, respectively. Since $\mathbb{Q}^A$ and $\mathbb{Q}^B$ are dense in A and B, they are dense as well. Also, since A and B have no endpoints, neither do $\mathbb{Q}^A$ and $\mathbb{Q}^B$. Then $\mathbb{Q}^A, \mathbb{Q}^B \models \delta$, and by Corollary 6.7, $\mathbb{Q}^A \cong \mathbb{Q}^B$.

Now, for every $a \in A$, form the set

$$\text{lc}(a) = \{\, b \in \mathbb{Q}^A \mid b <_A a \,\}.$$

($\text{lc}(a)$ corresponds to the lower Dedekind cut for a.) Then define

$$\text{DC}(A) = \{\, \text{lc}(a) \mid a \in A \,\},$$

ordered by $\subseteq$. Then we claim that $\langle A, < \rangle \cong \langle \text{DC}(A), \subseteq \rangle \cong \langle \text{DC}(B), \subseteq \rangle \cong \langle B, < \rangle$.

First, note that lc is an isomorphism from $(A, <)$ to $\langle \text{DC}(A), \subseteq \rangle$.

Now we must exhibit an isomorphism between $\langle \text{DC}(A), \subseteq \rangle$ and $\langle \text{DC}(B), \subseteq \rangle$. Let $f : \mathbb{Q}^A \to \mathbb{Q}^B$ be an isomorphism. Then define a map $F : \text{DC}(A) \to \text{DC}(B)$ which sends X to $f[X]$. We must show that F is well-defined: it is not immediate that $f[\text{lc}(a)] \in \text{DC}(B)$. Note that there must be some $a' \in \mathbb{Q}^A$ greater than a. Moreover, since f is order-preserving, $f(a')$ is an upper bound of $f[\text{lc}(a)]$. Therefore, since B is order-complete, there exists a least upper bound $b \in B$ of $f[\text{lc}(a)]$. We claim that $f[\text{lc}(a)] = \text{lc}(b)$. First, if $x \in \text{lc}(a)$, then $f(x) \in \text{lc}(b)$ since $\text{lc}(b)$ contains all elements of $\mathbb{Q}^B$ less than b. If $y \in \text{lc}(b)$, then there must

be some $x \in \mathrm{lc}(a)$ for which $f(x) = y$; otherwise, since f is onto, there would have to be some $x' \geq a$ for which $f(x') = y$, but this would contradict the fact that f is order-preserving.

F is order-preserving since $X \subseteq Y \implies f[X] \subseteq f[Y]$.

We can similarly define $F^{-1} : \mathrm{DC}(B) \to \mathrm{DC}(A)$ which sends X to $f^{-1}[X]$; a parallel argument shows that F^{-1} is well-defined and order-preserving.

Finally, we note that since f is an injection, $f^{-1}[f[X]] = X$, so F and F^{-1} are inverse, and therefore F is an isomorphism. ∎

Remark. lc in the preceding proof is an injection from $\mathbb{R}$ to $\mathcal{P}(\mathbb{Q})$; therefore, $\mathrm{card}(\mathbb{R}) \leq 2^{\aleph_0}$.

Definition 6.11 (Cantor set)**.** Let $C = \{0, 2\}^\omega$. Then $|C| = 2^{\aleph_0}$.

Now for each $f \in C$, form the sum

$$\sum_{i=1}^{\omega} f(i) \cdot 3^{-i}.$$

This gives the set of real numbers whose "trinary" expansions omit the digit 1.

Remark. We can also construct this set by taking $D_0 = [0, 1]$, D_1 to be D_0 without the middle 1/3, D_2 to be D_1 with the middle 1/3 removed from each of its subintervals, and so on recursively. Then $C = \bigcap_{n \in \omega} D_n$.

Note that C is a closed set with maximal cardinality which is nowhere dense!

If each element of C defines a distinct real number, then we see that $2^{\aleph_0} \leq \mathrm{card}(\mathbb{R})$. Since we showed in the proof of Theorem 6.10 that $\mathrm{card}(\mathbb{R}) \leq 2^{\aleph_0}$, in fact $\mathrm{card}(\mathbb{R}) = 2^{\aleph_0}$.

Definition 6.12. A subset of $\mathbb{R}$ is *open* if it is a union of open intervals. A subset is *closed* if it is the complement of an open set.

Remark. Open sets form a *topology* on $\mathbb{R}$, since they include $\mathbb{R}$ and $\emptyset$ and are closed under arbitrary unions and finite intersections.

Note that $\mathbb{R}$ has a countable basis, namely, the set of open intervals with rational endpoints.

Remark. Consider $|\mathcal{P}(\mathbb{R})| = 2^{2^{\aleph_0}} > 2^{\aleph_0}$. That's a lot of sets! The CH states that every element of $\mathcal{P}(\mathbb{R})$ is either countable or has the same cardinality as $\mathbb{R}$, but it seems difficult to get a handle on something quantifying over such a large set. Perhaps we can make better progress if we look at simpler classes of subsets of $\mathbb{R}$, for example, open sets. There are only $2^{\aleph_0}$ open sets, since each is a countable union of intervals from the countable basis of $\mathbb{R}$.

Lecture 8: The Real Line, Part II
February 11, 2009

Definition 6.13. $a \in X$ is *isolated in* X iff there is an open interval I for which $X \cap I = \{a\}$. Otherwise, a is a *limit point*.

Remark. Another way to state this is that a is isolated if it is not a limit point of X.

Definition 6.14. X is a *perfect set* iff X is closed and has no isolated points.

Remark. This definition sounds nice and tidy, but there are some very strange perfect sets. For example, the Cantor set is perfect, despite being nowhere dense!

Our goal will be to prove the Cantor-Bendixson theorem, *i.e.* the perfect set theorem for closed sets, that every closed uncountable set has a perfect subset.

Lemma 6.15. *If P is a perfect set and I is an open interval on $\mathbb{R}$ such that $I \cap P \neq \emptyset$, then there exist disjoint closed intervals $J_0, J_1 \subset I$ such that $\text{int}[J_0] \cap P \neq \emptyset$ and $\text{int}[J_1] \cap P \neq \emptyset$. Moreover, we can pick J_0 and J_1 such that their lengths are both less than any $\epsilon > 0$.*

Proof. Since P has no isolated points, there must be at least two points $a_0, a_1 \in I \cap P$. Then just pick $J_0 \ni a_0$ and $J_1 \ni a_1$ to be small enough. ∎

Lemma 6.16. *If P is a nonempty perfect set, then $P \sim \mathbb{R}$.*

Proof. We exhibit a one-to-one mapping $G : 2^\omega \to P$.

Note that 2^ω can be viewed as the set of all infinite paths in a full, infinite binary tree with each edge labeled by 0 or 1. We label each node in the tree by the sequence of labels on the path from the root to the node.

Now we associate an interval I_s to each node s, with the properties that

- I_s is closed,
- $I_s \cap P \neq \emptyset$,
- $I_{s,b} \subset I_s$,
- $I_{s,0} \cap I_{s,1} = \emptyset$, and
- $|I_s| < 1/(|s| + 1)$,

where $|I|$ denotes the length of interval I and $|s|$ denotes the length of sequence s.

In particular, if $\langle\rangle$ denotes the empty sequence, let $I_{\langle\rangle}$ be the closure of $I \cap P$ for some open interval I with length at most 1 whose intersection with P is nonempty. Then, given a set I_s satisfying the above properties, by Lemma 6.15 choose $I_{s,0}$ and $I_{s,1}$ to be disjoint closed subintervals of I_s shorter than $1/(|s|+2)$ whose intersection with P is nonempty.

Now, for all $f \in 2^\omega$, define

$$G(f) = \bigcap_{i \in \omega} I_{\overline{f}(i)},$$

where $\overline{f}(n) = \{f(0), f(1), \ldots, f(n)\}$. Actually, we are abusing notation a bit here: what we mean is that $G(f)$ is the unique member of the given intersection; we must show that this intersection does indeed result in a singleton set. This follows from the fact that we have an infinite intersection of nested, closed intervals of arbitrarily small length and that the real numbers are order-complete.

To see that $G(f) \in P$, note that $G(f)$ is an intersection of decreasing intervals, each of which has a nonempty intersection with P; if we pick one point from the intersection of each interval with P, they form a sequence with limit $G(f)$, which is contained in P since P is closed.

Finally, suppose $f, f' \in 2^\omega$ with $f \neq f'$. Let $n \in \omega$ be the smallest index for which $f(n) \neq f'(n)$. Then $I_{\overline{f}(n)} \cap I_{\overline{f'}(n)} = \emptyset$ by construction, and therefore $G(f) \cap G(f') = \emptyset$. This shows that G is injective. ∎

Theorem 6.17 (Cantor-Bendixson)**.** *If $C \subseteq \mathbb{R}$ is closed and uncountable, then there exists some perfect, nonempty $P \subseteq C$.*

Remark. In a sense, this is where set theory started. This proof is what motivated the development of transfinite ordinals, since it describes a recursive process that is not completed after the first limit stage.

Proof. Let $C \subseteq \mathbb{R}$ be closed. Define the *Cantor-Bendixson derivative*

$$C' = \{\, a \in C \mid a \text{ is a limit point of } C \,\}.$$

This operation maps closed sets to closed sets, since closed sets in $\mathbb{R}$ are those which contain all their limit points, and the derivative is monotone and retains all limit points. Then define

$$\begin{aligned} C_0 &= C \\ C_{\alpha+1} &= (C_\alpha)' \\ C_\lambda &= \bigcap_{\beta<\lambda} C_\beta \qquad (\lim(\lambda)). \end{aligned}$$

Note that C_β is closed for all β by induction.

Claim: $C_\gamma = C_{\gamma+1}$ for some γ. For if not, $C_\alpha \neq C_\beta$ for any $\alpha \neq \beta$, since C is monotone. Then $C_{(-)}$ would be an injection $Ord \to \mathcal{P}(C)$, which is absurd.

Note that C_γ is perfect, since it consists solely of limit points and is closed. If $C_\gamma \neq \emptyset$, we are done.

We claim that C_γ cannot be $\emptyset$ since this would imply that C is countable. Consider $C_\beta - C_{\beta+1}$, which contains all the isolated points in C_β. That is, if $a \in C_\beta - C_{\beta+1}$, there exists an open interval $I_a \ni a$ such that $C_\beta \cap I_a = \{a\}$. In particular, we may choose I_a to be an open interval with rational endpoints.

Note that each I_a is distinct; otherwise, at the earliest stage when I_a arose, it would have contained more than one point. Therefore, we have an injection from C into the set of intervals with rational endpoints, which is countable. ∎

Remark. The above proof shows that every closed set can be decomposed into a perfect subset and a countable subset. (In fact, it turns out that every closed set can be *uniquely* so decomposed.)

Definition 6.18. The smallest γ in the above proof for which $C_\gamma = C_{\gamma+1}$ is called the *Cantor-Bendixson rank* of C, and the above proof shows that $\gamma < \aleph_1$.

Exercise: construct closed sets whose Cantor-Bendixson rank is strictly greater than ω. In fact, it can be shown that for every $\gamma < \aleph_1$, there exists a closed $C \subseteq \mathbb{R}$ with Cantor-Bendixson rank γ.

Corollary 6.19. *For every $C \subseteq \mathbb{R}$, if C is closed and uncountable then $C \sim \mathbb{R}$. This follows from Lemma 6.16 and Theorem 6.17.*

Remark. We might hope that every uncountable set has a perfect subset; this, of course, would resolve the CH. However...

Theorem 6.20. *There exists a set X with $\mathrm{card}(X) = 2^{\aleph_0} = \mathrm{card}(\mathbb{R} - X)$ such that for every perfect set P, $P \not\subseteq X$ and $P \not\subseteq \mathbb{R} - X$.*

Proof. We use the AC to construct X. Let $P_\alpha, \alpha < 2^{\aleph_0}$ be an ordering of the perfect sets (there are $2^{\aleph_0}$ perfect sets; see Lemma 6.21). Also, let x_α be an ordering of $\mathbb{R}$. Now define r_γ to be the real number with next-to-least index in the sequence x_α which comes after all r_β, $\beta < \gamma$, and for which $r_\gamma \in P_\gamma$. We can keep picking such r_γ since each P_α has cardinality $2^{\aleph_0}$ and therefore cannot be contained in any initial segment of the x_α's. ∎

Lemma 6.21. *There are $2^{\aleph_0}$ perfect sets.*

Proof. There are at least $2^{\aleph_0}$ perfect sets, since there is an injection from $\mathcal{P}(\mathbb{N})$ to the set of all perfect sets: for each set of naturals, identify each natural with a small closed interal containing it, and take the union. There are at most $2^{\aleph_0}$ perfect sets since there are $2^{\aleph_0}$ closed sets (which, in turn, follows from the fact that any closed set can be expressed as a countable intersection of rational intervals). ∎

Lecture 9: Relative Consistency I
February 16, 2009

7 The Axiom of Regularity

Remark. We will now move more towards logic. We want to be able to show various independence results, such as that the consistency of ZF implies the consistency of ZF + AC + CH (and also ZF + AC + ¬CH). In some sense we can think of this as the "metamathematics" of set theory.

Definition 7.1 (Axiom of Regularity (Reg))**.** Every set has an $\in$-minimal element. Formally:

$$\forall x.(\exists y.y \in x) \implies \exists y.(y \in x \wedge (\forall z.z \in y \implies z \notin x)).$$

Remark. This axiom implies that we cannot have a set x which is an element of itself; then the set $\{x\}$ does not satisfy the axiom. We also cannot have a cyclic chain of inclusions $x_1 \in x_2 \in x_3 \in \cdots \in x_1$, or an infinite descending chain $x_1 \ni x_2 \ni x_3 \ni \dots$; in either case, the set $\{x_1, x_2, x_3, \dots\}$ fails to satisfy the axiom of regularity.

Note that we did not particularly need this axiom for the theory of *Ord*, $\mathbb{Q}$, $\mathbb{R}$, and so on, since all of those classes are well-founded by definition. But it will become convenient to restrict ourselves to well-founded sets when talking about models of set theory.

One question to ask ourselves is, given Reg, could we still have non-well-founded classes? The answer, it turns out, is no.

Definition 7.2. The *transitive closure* $TC(x)$ of a set x is defined as follows:

$$\begin{aligned} x_0 &= x \\ x_{n+1} &= \bigcup x_n \\ TC(x) &= \bigcup_{n \in \omega} x_n. \end{aligned}$$

Lemma 7.3. *$TC(x)$ is the $\subseteq$-least transitive set y such that $x \subseteq y$.*

Proof. First we show that $TC(x)$ is transitive. Suppose $y \in TC(x)$, and $z \in y$. By definition, $y \in x_n$ for some $n \in \omega$. But then $z \in x_{n+1}$; therefore, $TC(x)$ is transitive.

Now, if $x \subseteq y$ and y is transitive, we will show that $TC(x) \subseteq y$. It suffices to show that $x_n \subseteq y$ for all n, which we show by induction. The base case holds by assumption. For the inductive case, suppose $x_m \subseteq y$. Then if $z \in x_{m+1}$, by definition, $z \in z' \in x_m$ for some z'; but then, since $x_m \subseteq y$ and y is transitive, $z \in y$. ∎

Lemma 7.4 (Regularity for classes)**.**

$$\exists x.\varphi(x) \implies \exists x.(\varphi(x) \wedge \forall y.(\varphi(y) \implies y \notin x))$$

Proof. Suppose φ is some predicate, and that $\varphi(u)$ holds. Then define

$$z = \{\, x \mid x \in TC(u) \wedge \varphi(x) \,\}.$$

If z is empty, then u is $\in$-minimal for φ. Otherwise, note that z is a set by comprehension, so by Reg, it has an $\in$-minimal element, call it y. Then y is $\in$-minimal for φ. For if $q \in y$ and $\varphi(q)$, then $q \in TC(u)$ by transitivity of $TC(u)$, and hence $q \in z$. But this contradicts the minimality of y. ∎

Definition 7.5. Recall the definition of the transfinite hierarchy of sets, V:

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

We write $V(x)$ if and only if there is some α for which $x \in V_\alpha$.

Definition 7.6 (Rank)**.** The *rank* of a set x, denoted $\operatorname{rank}(x)$, is the least α for which $x \in V_{\alpha+1}$.

Theorem 7.7. *Under ZFC, the transfinite hierarchy of sets contains all sets. Formally,*

$$\mathrm{ZFC} \vdash \forall x.V(x).$$

Proof. Suppose there is some set x for which $\neg V(x)$. Let u be the $\in$-minimal such set (by Regularity). Then for every $w \in u$, there is some α for which $w \in V_\alpha$. Therefore, rank is a functional relation on u. Now consider $\sup(\operatorname{rank}[u]) = \beta$; we claim that $u \subseteq V_{\beta+1}$. Consider $x \in u$; by definition, $\beta \geq \operatorname{rank}(x)$, so $x \in V_{\beta+1}$, since the V_α are cumulative. Therefore $u \subseteq V_{\beta+1}$, a contradiction. ∎

Remark. This shows that every class which is bounded in rank is a set. Conversely, every class which is not bounded in rank is not a set.

We will now start in on proving some relative consistency results.

Theorem 7.8. *If ZF without Regularity is consistent, then so is ZF.*

Remark. We will show this by proving that from ZF without Regularity, we can prove the "relativization" of the ZF axioms to V.

Definition 7.9. The *relativization* of a formula φ to V, denoted φ^V, is defined as follows. All atomic formulas ($\in$, $=$) translate to themselves. $(-)^V$ commutes past $\wedge$, $\vee$, and $\neg$. The only interesting cases are $\forall$ and $\exists$:

$$\begin{aligned} [\exists x.\varphi]^V &= \exists x.V(x) \wedge \varphi^V \\ [\forall x.\varphi]^V &= \forall x.V(x) \implies \varphi^V \end{aligned}$$

That is, we change quantifiers into "bounded quantifiers" which have a universe of V.

$(\mathrm{ZF})^V$ indicates the set of axioms of ZF, each relativized to V.

Definition 7.10. Δ_0 is the smallest set of formulas containing atoms ($x \in y$ or $x = y$) and closed under connectives and bounded quantifiers (*e.g.* $\forall x \in z.\varphi$).

Definition 7.11. φ is *absolute* for M iff for all $\overline{x} \in M$,

$$\varphi^M(\overline{x}) \iff \varphi(\overline{x}).$$

Remark. As usual, we take $\overline{x} \in M$ to indicate a sequence of elements of M.

Lemma 7.12. *If M is transitive and φ is Δ_0, then φ is absolute for M.*

Proof. By structural induction on φ. First, if φ is an atom, then $\varphi^M(\overline{x}) = \varphi(\overline{x})$. If the top-level constructor of φ is $\wedge$, $\vee$, or $\neg$, the result follows immediately by definition of relativization and the induction hypothesis.

Now suppose φ is of the form $\exists x \in a.\varphi'$, that is, $\exists x.x \in a \wedge \varphi'$. By the induction hypothesis, we know that φ' is absolute for M. Note that

$$\varphi^M = \exists x.M(x) \wedge x \in a \wedge \varphi'^M.$$

$\left[\varphi^M(\overline{x}) \implies \varphi(\overline{x}).\right]$ Let $\overline{x} \in M$, and suppose $\varphi^M(\overline{x})$; we wish to show that $\varphi(\overline{x})$. Let y be the set that witnesses $\varphi^M(\overline{x})$. Then we can show that y also witnesses $\varphi(\overline{x})$. We know that $y \in a$ from $\varphi^M(\overline{x})$. However, φ' may contain x free; we must show $\varphi'(\overline{x}, y)$. This follows from the induction hypothesis if $y \in M$: but $\varphi^M(\overline{x})$ gives us $M(y)$.

$\left[\varphi(\overline{x}) \implies \varphi^M(\overline{x}).\right]$ Now suppose $\varphi(\overline{x})$, and let y be the witness. y is also a witness of $\varphi^M(\overline{x})$; the argument is similar, except we also need to show that $M(y)$ holds. We know that $y \in a$; but a is free in φ, so in $\varphi(\overline{x})$ it has been replaced by some element of $\overline{x}$, which is in M by assumption. M is transitive, so this implies that $y \in M$ as well.

Finally, suppose φ is of the form $\forall x \in a.\varphi'$, that is, $\forall x.x \in a \Rightarrow \varphi'$. Then we have

$$\varphi^M = \forall x.M(x) \Rightarrow x \in a \Rightarrow \varphi'^M.$$

$\left[\varphi^M(\overline{x}) \implies \varphi(\overline{x}).\right]$ Omitted. (For now. Maybe.) ∎

Lecture 10: A Digression on Absoluteness
February 18, 2009

8 A digression

Remark. An example of a formula which is *not* Δ_0 is the formula $\varphi(x)$ which states $\text{card}(x) = \omega$, that is,

$$\exists f.(f : \omega \xrightarrow[\text{onto}]{\text{1-1}} x). \tag{1}$$

Note that $\exists f$ is an *unbounded* quantifier.

Moreover, it is the case that φ is not absolute for transitive universes, demonstrating (by Lemma 7.12) that it is not possible to find *any* Δ_0 formula expressing the same property. We will spend the rest of the lecture exploring why.

Definition 8.1. B is an *elementary substructure* (or *elementary submodel*) of A, denoted $B \preceq A$, iff for all formulas $\varphi(\overline{x})$ and $\overline{b} \in B$,

$$B \models \varphi[\overline{b}] \iff A \models \varphi[\overline{b}].$$

Definition 8.2. A and B are *elementarily equivalent*, denoted $A \equiv B$, iff for all φ,

$$A \models \varphi \iff B \models \varphi.$$

Remark. For example, consider the structures $A = \langle \omega, < \rangle$ and $B = \langle \omega - \{0\}, < \rangle$. These are isomorphic, and therefore $A \equiv B$. However, it is not the case that $B \preceq A$: for example, if $\varphi(x)$ denotes "x has no predecessor," then $B \models \varphi(1)$ but $A \not\models \varphi(1)$. (Also, $A \not\preceq B$ since A is not a subset of B.)

Lemma 8.3 (Mostowski's Collapsing Lemma)**.** *If $A = \langle A, E^A \rangle$ is a well-founded extensional model of ZF, then A is isomorphic to a transitive set.*

Proof. Suppose $\langle A, E^A \rangle$ is a well-founded, extensional model of ZF. Then define $f : A \to V$ by

$$f(a) = \{\, f(b) \mid E^A(b, a) \,\}.$$

(Note that we may recursively define f in this way since $\langle A, E^A \rangle$ is well-founded.) Then we must show that $f[A]$ is transitive, and that f is an isomorphism.

First, we show that $f[A]$ is transitive. Let $x \in y \in f[A]$. Then $y = f(a)$ for some $a \in A$, and $y = \{\, f(b) \mid E^A(b, a) \,\}$. Therefore, $x = f(b)$ for some b with $E^A(b, a)$, which means that $x \in f[A]$.

Now, we must show f is an isomorphism between A and $f[A]$. Clearly it is surjective, so we need only show it is structure-preserving. Suppose $E^A(b, a)$; then $f(b) \in f(a)$ by definition of $f(a)$. ∎

Remark. We interrupt this lecture to bring you the following digression within a digression.

> *Remark.* In the statement of Lemma 8.3, why do we need to state that A is a *well-founded* model of ZF? Doesn't this follow from the axiom of regularity and the fact that it is a model?
>
> The somewhat surprising answer is: no! "Just because A *thinks* it is well-founded..." In fact, we can actually show the following theorem.
>
> **Theorem 8.4.** *If A is an infinite structure with arbitrarily long finite chains, then there exists a non-well-founded structure B such that $B \equiv A$.*
>
> To prove this theorem, we first need a few more tools.
>
> **Theorem 8.5** (Compactness of first-order logic (Gödel))**.** *For any set of first-order sentences T, if every finite $S \subseteq T$ is satisfiable, then T is satisfiable.*
>
> *Remark.* Gödel first showed this as a corollary to his completeness theorem for first-order logic.
>
> **Theorem 8.6** (Completeness of first-order logic (Gödel))**.** *For every formula φ of first-order logic, if $T \models \varphi$, then $T \vdash \varphi$.*
>
> *Proof.* We prove that Theorem 8.5 is a corollary to Theorem 8.6, by showing the contrapositive. Suppose that T is not satisfiable. Then $T \models \varphi \wedge \neg\varphi$, vacuously; so, by Theorem 8.6, $T \vdash \varphi \wedge \neg\varphi$. Proofs must be finite, so the proof must use only a finite set S of formulas in T. Hence $S \vdash \varphi \wedge \neg\varphi$, and by the soundness of first-order logic, $S \models \varphi \wedge \neg\varphi$. Therefore S is not satisfiable. ☒
>
> *Remark.* There are actually at least three other ways to show Theorem 8.5. One was shown by some guy using structures with constants, or something like that. One was shown by some other guy using ultraproducts, whatever those are (we might see this later in the course). Finally, there are topological methods involving scary things named for people.
>
> *Proof.* We are now in a position to prove Theorem 8.4. Suppose A is a structure with arbitrarily long chains. Now define
>
> $$T = Th(A) \cup \{\, E(c_{n+1}, c_n) \mid n \in \omega \,\},$$
>
> where E is the relation of A, the c_i are new constant symbols, and $Th(A) = \{\, \varphi \mid A \models \varphi \,\}$. Since A contains arbitrarily long finite chains, any finite subset of T is satisfiable by assigning appropriate elements of A to the c_i. By Theorem 8.5, T is satisfiable, that is, there exists a structure B such that $B \models T$. Clearly, B cannot be well-founded, because it contains an

infinite decreasing chain. Note that $A \models \varphi \implies B \models \varphi$ by construction. The converse is also true, which we can show by contradiction: if $B \models \varphi$ but $A \not\models \varphi$, then $A \models \neg\varphi$, implying that $B \models \neg\varphi$, a contradiction. Thus, $A \equiv B$. ∎

Remark. This means that ZF—even with the Axiom of Regularity—has non-well-founded models! Note, however, that any infinitely descending chain in such a model is *not* represented by an element in the universe.

Consider also the naturals with addition, multiplication, successor, and zero, ordered by $<$, which is a well-founded relation. The preceding theorem shows that there are models of these axioms which are not well-founded! Such a model has "non-standard naturals"; each of these have successors and predecessors which are also non-standard, so each "sprouts" a "$\mathbb{Z}$-chain". Similarly, each of the elements in a $\mathbb{Z}$-chain is $a+n$ for some standard n, $a+a$ must sprout a different $\mathbb{Z}$-chain, and so on...

Remark. And now, back to your regularly scheduled digression.

Theorem 8.7 (Löwenheim-Skolem)**.** *If $A = \langle A, E^A \rangle$ is a structure (that is, a set with a binary relation) such that $A \models T$, then for all countable $X \subseteq A$, there is some countably infinite B with $X \subseteq B \subseteq A$, and $B \preceq A$.*

Proof. (Deferred to a later lecture.) ∎

Remark. With the machinery we have now developed, we can show that equation (1) is not absolute for all transitive universes—that is, it could be true in some universe, but *not* true in some relativization of that universe which is still a model.

Theorem 8.8. *There is some transitive universe M for which*

$$\varphi(x) = \exists f.(f : \omega \xrightarrow[onto]{1\text{-}1} x)$$

is not absolute.

Proof. Let $\langle A, E \rangle$ be a well-founded, extensional model of ZF. By Löwenheim-Skolem, we can find a countable model of ZF, B, which is an elementary submodel of A (and hence well-founded and extensional). Then, by Mostowski, B is isomorphic to a transitive set C. Since C is a model of ZF, it must contain some element x satisfying the formula "$x = \mathcal{P}(\omega)$", and it must be the case that

$$C \models \neg\exists f.(f : \omega \xrightarrow[\text{onto}]{1\text{-}1} x)$$

(this is just Cantor's Theorem). But C is countable, and since C is transitive, x must be countable also. Hence, "countableness" is not an absolute property. ∎

Remark. This is known as Skolem's Paradox, and gives additional insight into the limits of first-order logic to express properties of sets.

Lecture 11: The Löwenheim-Skolem Theorem
February 23, 2009

Remark. We now return to prove the Löwenheim-Skolem theorem from the previous lecture. In fact, we will prove a slightly more general version. But first, we need a lemma.

Lemma 8.9 (Tarski-Vaught $\preceq$-criterion)**.** *If $B \subseteq A$, and for all $\overline{b} \in B$ and formulas $\varphi(\overline{x}, y)$, $A \models \exists x.\varphi[\overline{b}]$ implies that there is a $b' \in B$ such that $A \models \varphi[\overline{b}, b']$, then $B \preceq A$.*

Proof. We show that

$$B \models \varphi[\overline{b}] \iff A \models \varphi[\overline{b}]$$

for all formulas φ by induction on the structure of φ. Without loss of generality, we may assume that φ does not contain $\forall$ (we can always translate $\forall$ into $\neg\exists\neg$).

- If φ is an atom, this follows from the definition of $\subseteq$ on structures.
- If $\varphi = \varphi_1 \wedge \varphi_2$, by the inductive hypothesis we know that $B \models \varphi_i[\overline{b}] \iff A \models \varphi_i[\overline{b}]$ for $i = 1, 2$. Then it is not hard to see that B satisfies $(\varphi_1 \wedge \varphi_2)[\overline{b}] = \varphi_1[\overline{b}] \wedge \varphi_2[\overline{b}]$ if and only if A does.
- The arguments for $\vee$ and $\neg$ are similar.
- If $\varphi = \exists y.\theta$. First, suppose $B \models \exists y.\theta[\overline{b}]$, and $b' \in B$ witnesses this. Then $B \models \theta[\overline{b}, b']$, which by the inductive hypothesis implies that $A \models \theta[\overline{b}, b']$, and hence that $A \models \exists y.\theta[\overline{b}]$.

  Conversely, suppose $A \models \exists y.\theta[\overline{b}]$. By assumption, there is a $b' \in B$ for which $A \models \theta[\overline{b}, b']$. But by the induction hypothesis, this shows that $B \models \theta[\overline{b}, b']$ and hence that $B \models \exists y.\theta[\overline{b}]$.

∎

Definition 8.10. Let A be a structure and $\varphi(\overline{x}, y)$ some formula. Then we may define a *Skolem function* f_φ for which

$$A \models \exists x.\varphi[\overline{c}, x] \implies A \models \varphi[\overline{c}, f_\varphi(\overline{c})].$$

The Skolem function f_φ picks a satisfier for the formula φ, assuming one exists.

Theorem 8.11 (Löwenheim-Skolem)**.** *If $A = \langle A, E^A \rangle$ is a structure (that is, a set with a binary relation) such that $A \models T$, then for all $X \subseteq A$, there is some B such that $X \subseteq B \subseteq A$, $B \preceq A$, and* $\operatorname{card}(B) = \aleph_0 \cdot \operatorname{card}(X)$.

Proof. First, form a set of Skolem functions

$$F = \{\, f_\varphi \mid \varphi \in T \,\}.$$

We note that F is countable, since T is (we assume a countable language). We define X_ω, the *Skolem hull of X in A*, as follows:

$$\begin{aligned} X_0 &= X \\ X_{i+1} &= \{\, f(\overline{c}) \mid \overline{c} \in X_i \text{ and } f \in F \,\} \\ X_\omega &= \bigcup_{i \in \omega} X_i \end{aligned}$$

In fact, X_ω is the desired B. That $X_\omega \preceq T$ follows by construction from the Tarski-Vaught criterion. Clearly $X \subseteq X_\omega \subseteq A$. Also, $\text{card}(X_\omega) \geq \aleph_0$, since it must satisfy all statements of the form "at least n elements exist"; $\text{card}(X_\omega) \leq \aleph_0 \cdot \text{card}(X)$, since it is a countable union of sets with size at most $\aleph_0 \cdot \text{card}(X)$. ∎

Remark. We now note that the Löwenheim-Skolem Theorem is one half of a more general observation about the sizes of models.

Theorem 8.12. *For any infinite structure A and cardinal $\kappa \geq \aleph_0$, there is a structure B such that $B \equiv A$ and* $\text{card}(B) = \kappa$.

Proof. Suppose $\text{card}(A) = \lambda$. If $\kappa \leq \lambda$, by Theorem 8.11 we can find some $B \preceq A$ with $\text{card}(B) = \kappa$, by forming the Skolem hull of some subset of A of cardinality κ; this implies that $B \equiv A$.

Conversely, suppose $\kappa > \lambda$. Let $\{\, C_\alpha \mid \alpha < \kappa \,\}$ be a set of new constant symbols. Now consider the set of formulas

$$T' = Th(A) \cup \{\, \neg(C_\alpha = C_\beta) \mid \alpha < \beta < \kappa \,\}.$$

Any finite subset of T' is satisfiable by A; hence, by compactness (Theorem 8.5), T' is satisfiable by some structure, call it B'. The cardinality of B' must be at least κ. Also, $B' \equiv A$ (with respect to the language without the extra constants C_α), and by Theorem 8.11 we may construct a $B \preceq B'$ with cardinality κ, and $B \equiv A$. ∎

Remark. For every *finite* A, on the other hand, there exists some φ_A such that $B \models \varphi_A$ if and only if $B \cong A$. That is, every finite structure can be characterized up to isomorphism in first-order logic. We can simply take φ_A to be a complete encoding of the relation on A.

Definition 8.13. A theory T is *κ-categorical* iff for all A and B, if $\text{card}(A) = \text{card}(B) = \kappa$ and $A \models T$ and $B \models T$, then $A \cong B$.

Remark. In other words, T is κ-categorical if it characterizes its models of cardinality κ up to isomorphism.

For example, $Th(\mathbb{Q}, <)$ is $\aleph_0$-categorical, but not $2^{\aleph_0}$-categorical, which we saw in a previous lecture.

There exist T which are not $\aleph_0$-categorical but are κ-categorical for every $\kappa > \aleph_0$. There are also trivial examples of T which are κ-categorical for all κ (for example, a set with the empty relation or total relation).

One might wonder whether there are T which are $\aleph_1$-categorical but not $\aleph_2$-categorical. The answer, as shown by M. Morley in the 1960's, is no.

Theorem 8.14 (Morley, 196?)**.** *If T is a complete, countable first-order theory, and T is κ-categorical for some $\kappa > \aleph_0$, then T is κ-categorical for all $\kappa > \aleph_0$.*

Remark. One might also wonder whether there is some countable structure A such that the second-order theory of A is not categorical? This question was shown by Ajtai to be independent of ZFC.

Lecture 12: Relative Consistency II
February 25, 2009

9 Relative consistency of Reg

We now finally return to prove Theorem 7.8:

Theorem 7.8. *If ZF without Regularity is consistent, then so is ZF.*

We'll first need a few more lemmas.

Lemma 9.1. *The rank hierarchy V (Definition 7.5) is transitive.*

Proof. By definition of V, it suffices to show that V_α is transitive for all ordinals α, which we show by transfinite induction.

- $V_0 = \emptyset$, which is vacuously transitive.
- By definition, $V_{\alpha+1} = \mathcal{P}(V_\alpha)$; by the inductive hypothesis we may assume V_α is transitive. Let $x \in V_{\alpha+1}$. Then $x \subseteq V_\alpha$. Now let $y \in x$; then $y \in V_\alpha$. But since V_α is transitive, this means that $y \subseteq V_\alpha$, and hence $y \in V_{\alpha+1}$.
- Now consider $V_\lambda = \bigcup_{\beta<\lambda} V_\beta$, where λ is a limit ordinal. Let $x \in V_\lambda$. Then $x \in V_\beta$ for some $\beta < \lambda$. Since V_β is transitive by the inductive hypothesis, if $y \in x$, then $y \in V_\beta$, and hence $y \in V_\lambda$. ∎

Remark. This immediately implies that the rank hierarchy is cumulative: $V_\alpha \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$, and since $V_{\alpha+1}$ is transitive, $V_\alpha \subseteq V_{\alpha+1}$ as well.

Lemma 9.2. *If all the elements of a set u are sets in the rank hierarchy, then so is u.*

Proof. Let α be the maximum rank of the elements of u; since the rank hierarchy is cumulative, $u \subseteq V_\alpha$. But then $u \in V_{\alpha+1}$. ∎

Lemma 9.3. *If x is in the rank hierarchy, so is $\mathcal{P}(x)$.*

Proof. Suppose $x \in V$. Therefore $x \subseteq V$, since V is transitive. Then by the previous lemma, every subset of x is in V. Applying the previous lemma again, we conclude that $\mathcal{P}(x) \in V$. ∎

Proof of Theorem 7.8. We must show that if we assume ZF - Reg, each of the axioms of ZF holds when relativized to V.

- Axiom of Extensionality. We must show

$$\left[\forall x.\forall y.((\forall z \in x.z \in y) \wedge (\forall z \in y.z \in x)) \Rightarrow (x = y)\right]^V.$$

By definition of $(-)^V$, this is equivalent to

$$\forall x \in V. \forall y \in V. \big[((\forall z \in x. z \in y) \wedge (\forall z \in y. z \in x)) \Rightarrow (x = y)\big]^V.$$

(where $\forall x \in V. \varphi$ is an abbreviation for $\forall x. V(x) \Rightarrow \varphi$). Let $x \in V$ and $y \in V$; then we must show the remainder of the formula for this particular x and y. However, note that this formula is Δ_0 and its free variables are in V (which is transitive), so by Lemma 7.12, its relativization holds iff the unrelativized version holds in the original universe—which is does, by the Axiom of Extensionality.

- Pairing. We must show

$$\big[\forall x. \forall y. \exists z. \forall w. (w \in z \Leftrightarrow (w = x \vee w = y))\big]^V,$$

that is,

$$\forall x \in V. \forall y \in V. \exists z \in V. \forall w \in V. (w \in z \Leftrightarrow (w = x \vee w = y)).$$

So, let $x, y \in V$, and let $z = \{x, y\}$, which is guaranteed to exist by the Axiom of Pairing. Note that $z \in V$, since its elements are (by Lemma 9.2). The remaining condition holds for all sets w by the Axiom of Pairing, so it certainly holds for all sets $w \in V$.

- Union. We must show

$$\big[\forall x. \exists y. \forall z. z \in y \Leftrightarrow (\exists w \in x. z \in w)\big]^V,$$

that is,

$$\forall x \in V. \exists y \in V. \forall z \in V. \big[z \in y \Leftrightarrow (\exists w \in x. z \in w)\big]^V,$$

noting that the part still in brackets is Δ_0. Let $x \in V$, and let $y = \bigcup x$ (which exists by the Axiom of Union). $y \in V$, again by Lemma 9.2. Finally, the formula in brackets holds for all sets z, so the relativized version certainly holds for all $z \in V$, since it is Δ_0.

- Power set. We must show

$$\big[\forall x. \exists y. \forall z. z \in y \Leftrightarrow (\forall w \in z. w \in x)\big]^V,$$

that is,

$$\forall x \in V. \exists y \in V. \forall z \in V. \big[z \in y \Leftrightarrow (\forall w \in z. w \in x)\big]^V.$$

Let $x \in V$, and let $y = \mathcal{P}(x)$. By Lemma 9.3, $y \in V$. The remainder of the argument is similar to the previous case.

- Infinity. We must show

$$\big[\exists x.\emptyset \in x \wedge (\forall y \in x.y \cup \{y\} \in x)\big]^V,$$

that is,

$$\exists x \in V.\big[\emptyset \in x \wedge (\forall y \in x.y \cup \{y\} \in x)\big]^V.$$

Note that the formula inside the brackets can be expressed as a Δ_0 formula. Let $x = \omega$, and note that it satisfies the Axiom of Infinity, and is in V (in particular, it is in $V_{\omega+1}$). Then we are done, since the remainder of the formula is Δ_0.

- Regularity. We must show

$$\big[\forall x.(\exists y \in x) \Rightarrow \exists y \in x.\forall z \in y.z \notin x\big]^V$$

(without using the Axiom of Regularity!). All but the $\forall x.$ is clearly Δ_0. So let $x \in V$, and suppose x is not empty. Pick y of minimal rank in x. Then $y \cap x = \emptyset$, since otherwise there would be some element of x which is also an element of y, contradicting the minimality of the rank of y.

- Separation. We must show that for all formulas φ,

$$\big[\forall \bar{t}.\forall x.\exists y.\forall z.z \in y \Leftrightarrow z \in x \wedge \varphi(z, \bar{t})\big]^V,$$

that is,

$$\forall \bar{t} \in V.\forall x \in V.\exists y \in V.z \in y \Leftrightarrow z \in x \wedge \varphi^V(z, \bar{t}).$$

So, let $\bar{t}, x \in V$. Then let $y = \{\, z \in x \mid \varphi^V(z, \bar{t}) \,\}$, which exists by the Axiom of Separation. But all the elements of y are elements of $x \in V$, and therefore also elements of V since V is transitive; but then by Lemma 9.2, $y \in V$.

- Replacement. We must show that for all F,

$$(F \text{ is a functional relation})^V \Rightarrow (\forall x.\exists y.y = F[x])^V,$$

that is, more explicitly,

$$(\forall x.(\exists y.F(x,y) \wedge (\forall y, y'.F(x,y) \wedge F(x,y') \Rightarrow y = y')))^V \Rightarrow (\forall x.\exists y.y = F[x])^V.$$

So, we are given the fact that F^V is a functional relation when restricted to V, and that it sends every element of V to another element of V. Let $x \in V$. Now, invoking the Axiom of Replacement, we may conclude that the image of x under $F^V \restriction V$ is a set. However, since all the elements of x are elements of V (since V is transitive), this image is a set of elements of V, and hence in V. Furthermore, this image y should satisfy

$$(y = F[x])^V,$$

that is,

$$(\forall z.(z \in y \Leftrightarrow \exists w \in x.F(w,z)))^V,$$

but this is clearly satisfied by the image of x under $F^V \restriction V$.

- Choice. We must show that

$$\left[\forall x.(\forall y \in x.y \neq \emptyset) \Rightarrow \exists f.\,\mathrm{dom}(f) = x \wedge \forall y \in x.f(y) \in y\right]^V,$$

that is,

$$\forall x \in V.(\forall y \in x.y \neq \emptyset) \Rightarrow \exists f \in V.\,\mathrm{dom}(f) = x \wedge \forall y \in x.f(y) \in y.$$

So, suppose $x \in V$ and all the elements of x are nonempty. Then by the Axiom of Choice, there exists a choice function f in the universe which clearly satisfies the necessary conditions on f. Also, f consists of pairs of elements of x and elements of elements of x, all of which are in V by transitivity; since V contains pairs by construction, $f \in V$. ☒

Lecture 13: Strongly Inaccessible Cardinals
March 2, 2009

10 Strongly inaccessible cardinals and ZF

Recall the definition of a strongly inaccessible cardinal.

Definition 10.1. κ is *strongly inaccessible* (SI) iff κ is regular and κ is a strong limit (that is, $2^\lambda < \kappa$ for every $\lambda < \kappa$). (We can also place the restriction that $\kappa > \omega$, since ω would not make a very interesting strongly inaccessible cardinal.)

Lemma 10.2. *If κ is a strongly inaccessible cardinal, then for every $\beta < \kappa$, $\mathrm{card}(V_\beta) < \kappa$.*

Proof. By induction on β. The base case ($\beta = 0$) is obvious.

Suppose $\beta = \alpha + 1$, and by the inductive hypothesis $\mathrm{card}(V_\alpha) < \kappa$. Then $\mathrm{card}(V_\beta) = 2^{\mathrm{card}(V_\alpha)} < \kappa$ since κ is a strong limit ordinal.

Now suppose β is a limit ordinal, and by the inductive hypothesis $\mathrm{card}(V_\alpha) < \kappa$ for every $\alpha < \beta$. Then $\mathrm{card}(V_\beta) = \sup_{\alpha<\beta} \mathrm{card}(V_\alpha)$, since the V_α are monotonically increasing. If this is equal to κ, then $\alpha \mapsto \mathrm{card}(V_\alpha)$ is a cofinal map $\beta \to \kappa$—but this is a contradiction, since $\beta < \kappa$ and κ is regular. ∎

Theorem 10.3. *If κ is a strongly inaccessible cardinal, then $V_\kappa \models ZF$.*

Proof. Since κ is a limit ordinal greater than ω, it is easy to see that $V_\kappa \models Z$ (that is, ZF without the Axiom of Replacement). So it only remains to show that $V_\kappa \models$ Replacement.

Let F be a functional relation, and let $x \in V_\kappa$. Then we wish to show that $F[x] \in V_\kappa$. First, note that since κ is a limit ordinal, $x \in V_\beta$ for some $\beta < \kappa$. Then since V_β is transitive, $x \subseteq V_\beta$ and hence $\mathrm{card}(x) \leq \mathrm{card}(V_\beta) < \kappa$ by Lemma 10.2.

Now let $\gamma = \sup\{\, \mathrm{rank}(F(y)) \mid y \in x \,\}$. Hence $F[x] \in V_{\gamma+1}$, so it remains only to show that $\gamma < \kappa$. But if $\gamma = \kappa$, then $y \mapsto \mathrm{rank}(F(y))$ would be a cofinal map from x to κ, a contradiction since $\mathrm{card}(x) < \kappa$. ∎

Theorem 10.4. $ZF \nvdash \exists\kappa.SI(\kappa)$.

Remark. We can show this using Gödel's second incompleteness theorem: suppose ZF could show the existence of a strongly inaccessible cardinal. Then by Theorem 10.3, we could derive $ZF \vdash \exists\kappa.V_\kappa \models ZF$. But by the completeness theorem of first-order logic, this amounts to a proof of ZF's consistency within ZF, contradicting Gödel's second incompleteness theorem.

This proof is pithy but not very illuminating. We can actually give a more elementary proof that does not rely on any incompleteness theorems. First, we'll need a lemma about strong inaccessibility.

Lemma 10.5 (Absoluteness of SI)**.** *If λ is a limit ordinal and $\kappa \in V_\lambda$, then $SI(\kappa) \iff V_\lambda \models SI(\kappa)$.*

Proof. Unfolding the definition of SI, it suffices to show each of the following.

- $\text{ord}(\kappa) \iff V_\lambda \models \text{ord}(\kappa)$. Since we have the Axiom of Regularity, $\text{ord}(\kappa)$ simply reduces to the statement that κ is a transitive linear order, both of which are Δ_0 conditions.

- $\text{card}(\kappa) \iff V_\lambda \models \text{card}(\kappa)$. Recall that $\text{card}(\kappa)$ holds iff there is no f for which there exists some $\beta < \kappa$ such that $f : \beta \xrightarrow[\text{onto}]{\text{1-1}} \kappa$.

  First, suppose $\text{card}(\kappa)$, that is, there is no bijection in the universe between κ and some $\beta < \kappa$. If there is no such bijection in the universe, there isn't one in V_λ either, since the notion of being a bijection between β and κ is Δ_0.

  Now, suppose $V_\lambda \models \text{card}(\kappa)$, and suppose by way of contradiction that there is some f in the universe which is a bijection between κ and some $\beta < \kappa$. Note that $f \subseteq \beta \times \kappa \subseteq \mathcal{P}(\mathcal{P}(\beta \cup \kappa))$, so its rank is at most two greater than the rank of κ. But $\kappa \in V_\lambda$, and since λ is a limit ordinal, $\kappa \in V_\alpha$ for some $\alpha < \lambda$, and hence $f \in V_{\alpha+2} \subseteq V_\lambda$, which is a contradiction.

- $\text{cf}(\kappa) = \kappa \iff V_\lambda \models \text{cf}(\kappa) = \kappa$. We can also restate $\text{cf}(\kappa) = \kappa$ as the fact that there is no ordinal $\alpha < \kappa$ for which there exists a cofinal map $f : \alpha \to \kappa$.

  ($\Longrightarrow$) Suppose there is no ordinal $\alpha < \kappa$ in the universe for which there exists a cofinal map $f : \alpha \to \kappa$. Then there is no such ordinal in V_λ, either, since the notion of being a cofinal map from $\alpha \to \kappa$ is absolute for V_λ (this is because $\alpha, \kappa \in V_\lambda$; the notion of being a functional relation from α to κ is absolute for V_λ; and the predicate defining what it means to be a *cofinal* map only has to talk about union, which lowers rank).

  ($\Longleftarrow$) Suppose that $V_\lambda \models \text{cf}(\kappa) = \kappa$, and suppose by way of contradiction that there is some $\alpha < \kappa$ and a cofinal map $f : \alpha \to \kappa$. Clearly $\alpha \in V_\lambda$. It is also easy to see that $f \in V_\lambda$ by the same argument as in the previous case.

- κ is a strong limit cardinal $\iff V_\lambda \models \kappa$ is a strong limit cardinal.

  First, suppose κ is a strong limit cardinal. This means that $2^\iota < \kappa$ for every cardinal $\iota < \kappa$, which is the case if and only if, for every $\iota < \kappa$, there is an injection $f : \mathcal{P}(\iota) \xrightarrow{\text{1-1}} \kappa$. By the usual rank argument, $f \in V_\lambda$.

  Now suppose $V_\lambda \models (\kappa$ is a strong limit cardinal), which means that for every cardinal $\iota < \kappa$, there is some $f \in V_\lambda$ such that $f : \mathcal{P}(\iota) \xrightarrow{\text{1-1}} \kappa$. But then for each ι, that f is evidence in the universe that $2^\iota < \kappa$; hence κ is a strong limit cardinal.

- κ is uncountable $\iff V_\lambda \models \kappa$ is uncountable.

  First, suppose κ is uncountable; then there does not exist any function $f : \kappa \xrightarrow{1\text{-}1} \omega$. Then in particular, there does not exist any such function in V_λ, since being an injection from κ into ω is absolute for V_λ.

  Now, suppose $V_\lambda \models \kappa$ is uncountable. By way of contradiction, suppose there is some f in the universe with $f : \kappa \xrightarrow{1\text{-}1} \omega$. By an easy rank argument (noting that κ uncountable implies $\lambda > \omega$), $f \in V_\lambda$.

□

Proof of Theorem 10.4. Suppose that ZF can show the existence of a strongly inaccessible cardinal. Then there must be a smallest such cardinal λ, that is,

$$ZF \vdash \exists\lambda.(SI(\lambda) \wedge \forall\nu < \lambda.\neg SI(\nu)).$$

So $V_\lambda \models ZF$, and in particular, it must be the case that $V_\lambda \models \exists\kappa.SI(\kappa)$. So, there must be some $\kappa < \lambda$ for which $V_\lambda \models SI(\kappa)$. However, we know by Lemma 10.5 that SI is absolute for V_λ, so $SI(\kappa)$, contradicting the fact that λ is the smallest such cardinal. □

Lecture 14: Midterm exam review
March 16, 2009

11 Midterm exam review

Theorem 11.1 (Problem 6)**.** *For all ordinals α and β, if $\alpha < \beta$ and $V_\alpha \preceq V_\beta$, then $V_\alpha \models ZF$.*

Proof. First, we note that if $\omega < \alpha$ and $\lim(\alpha)$, then $V_\alpha \models Z$ (ZF without Replacement).

We can also easily show that α must be a limit ordinal greater than ω. First, if $\alpha = \gamma + 1$, then $\gamma \in V_\alpha$ but $\{\gamma\} \notin V_\gamma$. However, since $\alpha < \beta$, γ and $\{\gamma\}$ are both elements of V_β; this is a contradiction since $V_\alpha \preceq V_\beta$, and in particular must satisfy the formula stating that $\{\gamma\}$ exists. Second, if $\alpha = \omega$, then V_β satisfies the Axiom of Infinity but V_α does not, another contradiction.

So, it remains only to show that if α is a limit ordinal greater than ω, $\alpha < \beta$, and $V_\alpha \preceq V_\beta$, then V_α satisfies Replacement. Suppose f is a functional relation in V_α and $z \in V_\alpha$. Then for every $y \in z$, $f(y) \in V_\alpha$, and therefore $f[z] \in V_{\alpha+1} \subseteq V_\beta$. But then V_α must satisfy the formula stating that the image of z under f is a set. ∎

Remark. As an aside, we can also show that the α in the above theorem must actually be a strong limit cardinal; left as an exercise.

Remark. There was other stuff in this lecture having to do with more specific points from the exam. We also started into discussing problem 3, which is to show that ZF has no finite axiomatization. See the next lecture notes for the beginning of this.

Lecture 15: The Reflection Principle
March 18, 2009

12 ZF is not finitely axiomatizable

Definition 12.1. A sequence of sets indexed by ordinals, M_α, is a *cumulative hierarchy* iff

1. $M_\alpha \subseteq M_{\alpha+1} \subseteq \mathcal{P}(M_\alpha)$, for all α, and
2. $\bigcup_{\alpha<\lambda} M_\alpha = M_\lambda$, for $\lim(\lambda)$.

Remark. For example, V (the rank hierarchy) is a cumulative hierarchy, as is L (the constructible hierarchy, to be covered later). Generally, if the sequence M_α is a cumulative hierarchy, we write $M(x)$ to denote the predicate $\exists\alpha.x \in M_\alpha$.

Definition 12.2. A class of ordinals C is closed unbounded (abbreviated *club*) iff

- it is *closed*, that is, $C(\lambda)$ holds for limit ordinals λ whenever, for every $\beta < \lambda$, there is some $\beta < \gamma < \lambda$ with $C(\gamma)$; and
- it is *unbounded*, that is, for every ordinal α there exists some ordinal $\beta > \alpha$ with $C(\beta)$.

Remark. A set of ordinals is club iff it is the image of a normal function.

Lemma 12.3. *If C and D are closed unbounded, then so is $C \cap D$.*

Proof. We must show that $C \cap D$ is closed, and unbounded.

- $C \cap D$ is closed. Let λ be a limit ordinal, and suppose that for every $\beta < \lambda$ there is some $\beta < \gamma < \lambda$ with $C(\gamma)$ and $D(\gamma)$. Then $\lambda \in C$ and $\lambda \in D$, hence $\lambda \in C \cap D$.
- $C \cap D$ is unbounded. Let β be an ordinal, and define a sequence $\langle \alpha_i \rangle$ such that $\beta < \alpha_0 < \alpha_1 < \ldots$ and $\alpha_{2i} \in C$, $\alpha_{2i+1} \in D$. We can construct such a sequence since C and D are unbounded. The sup of this sequence is larger than β, and in both C and D. ∎

Lemma 12.4. *For any map F which sends ordinals to ordinals, the class*

$$C = \{\, \alpha \mid \forall\beta.\beta < \alpha \Rightarrow F(\beta) < \alpha \,\}$$

is closed unbounded.

Remark. This seems quite magical! It is not even obvious that C should be nonempty. In some sense it asserts that infinitely many "strong limits" exist with respect to any map F, not just $\alpha \mapsto 2^\alpha$.

Proof. We must show that C is closed, and that it is unbounded.

- C is closed. Suppose $\lim(\lambda)$ and there is some increasing sequence ξ below λ contained in C. Pick any $\beta < \lambda$. Then since ξ is increasing, and λ is a limit ordinal, there must be some $\beta < \alpha < \lambda$ with $\alpha \in \xi$, that is, $\alpha \in C$. But then $F(\beta) < \alpha < \lambda$, so $\lambda \in C$.

- C is unbounded. Suppose γ is an ordinal; we wish to show there is some $\delta > \gamma$ with $\delta \in C$.

  Define

$$\begin{aligned} \gamma_0 &= \gamma \\ \gamma_{n+1} &= 1 + \sup_{\alpha<\gamma_n} \{F(\alpha)\} \\ \delta &= \sup_{n\in\omega} \{\gamma_n\}. \end{aligned}$$

  Now pick $\beta < \delta$; we wish to show that $F(\beta) < \delta$, from which it will follow that $\delta \in C$. By definition of δ, there is some n for which $\beta < \gamma_n$. But then $F(\beta) \leq \sup_{\alpha<\gamma_n} \{F(\alpha)\} < \gamma_{n+1} \leq \delta$. ∎

Theorem 12.5 (Reflection principle)**.** *For every cumulative hierarchy M and formula $\varphi(x_1, \ldots, x_n)$, there is a closed unbounded class C of ordinals such that for every $\alpha \in C$,*

$$\forall \overline{x} \in M_\alpha . \varphi^{M_\alpha}(\overline{x}) \Leftrightarrow \varphi^M(\overline{x}).$$

Remark. If $M = V$, $\varphi^M = \varphi^V = \varphi$ under Regularity; hence every formula φ is reflected by some closed unbounded class of ranks.

Definition 12.6. A theory T is *reflexive* if $T \vdash Con(\varphi)$ for every $\varphi \in Conseq(T)$ (where Con denotes "is consistent" and $Conseq(T)$ denotes the set of all formulas derivable in T).

Remark. By Gödel's second incompleteness theorem, a reflexive theory (which is strong enough for the theorem to apply) can't be finitely axiomatizable. If it were, there would be some formula (the conjunction of the axioms) from which the entire theory would follow; but since the theory is reflexive it would then be able to prove its own consistency.

Moreover, the reflection principle implies that ZF is reflexive, and hence is not finitely axiomatizable. However, we will later give a more set-theoretic proof of this using the reflection principle, without appealing to Gödel.

Proof of Theorem 12.5. By induction on φ. (We may assume that $\forall$ and $\vee$ are encoded in terms of $\exists$, $\neg$, and $\wedge$.)

- If φ is an atomic formula ($x_1 \in x_2$ or $x_1 = x_2$) we may take C to be the class of all ordinals. (Relativization is the identity on atomic formulas.)

- $\varphi = \neg\theta$. By the inductive hypothesis, there is a club class C_θ corresponding to θ; we may take $C_\varphi = C_\theta$, since the condition for φ is equivalent to the condition for θ.

- $\varphi = \theta \wedge \psi$. If C_θ and C_ψ are the club classes from the inductive hypotheses, then $C_\varphi = C_\theta \cap C_\psi$ (which is club by Lemma 12.3) reflects φ, since if $\theta^{M_\alpha} \Leftrightarrow \theta^M$ and $\psi^{M_\alpha} \Leftrightarrow \psi^M$ both hold, then so does $\theta^{M_\alpha} \wedge \psi^{M_\alpha} \Leftrightarrow \theta^M \wedge \psi^M$, which is equivalent to $(\theta \wedge \psi)^{M_\alpha} \Leftrightarrow (\theta \wedge \psi)^M$.

- $\varphi = \exists y.\zeta(\overline{x}, y)$; let C_ζ reflect $\zeta(\overline{x}, y)$ by the inductive hypothesis.

  Now define $G(\overline{x})$ to be the least α such that there is some $y \in M_\alpha$ with $\zeta^M(\overline{x}, y)$, or 0 if there is no such α. In other words, for a given $\overline{x}$, $G(\overline{x})$ is the smallest rank that reflects φ for that particular $\overline{x}$.

  Furthermore, define

  $$F(\beta) = \sup\{\, G(\overline{x}) \mid \overline{x} \in M_\beta \,\}.$$

  Now, we claim that $C_\varphi = C_\zeta \cap \{\, \alpha \mid \lim(\alpha) \,\} \cap \{\, \alpha \mid \forall\beta.\beta < \alpha \Rightarrow F(\beta) < \alpha \,\}$ satisfies the requirements of the reflection principle. Note that C_φ is club by Lemmas 12.3 and 12.4.

  It remains only to show that C_φ reflects φ, that is, for every $\alpha \in C_\varphi$,

  $$\forall \overline{x} \in M_\alpha.(\exists y.\zeta(\overline{x}, y))^{M_\alpha} \Leftrightarrow (\exists y.\zeta(\overline{x}, y))^M.$$

  So, suppose $\alpha \in C_\varphi$ and $\overline{x} \in M_\alpha$.

  ($\Rightarrow$) We are given $(\exists y.\zeta(\overline{x}, y))^{M_\alpha}$, that is, there is some $y \in M_\alpha$ such that $\zeta^{M_\alpha}(\overline{x}, y)$ holds. Clearly $y, \overline{x} \in M$, and since $\alpha \in C_\zeta$, we conclude that $\zeta^M(\overline{x}, y)$ holds as well.

  ($\Leftarrow$) We have $(\exists y.\zeta(\overline{x}, y))^M$, that is, there is some $y \in M$ such that $\zeta^M(\overline{x}, y)$; we wish to show that there is some $y' \in M_\alpha$ such that $\zeta^{M_\alpha}(\overline{x}, y')$.

  Since $\alpha \in C_\varphi$, it is a limit ordinal, and therefore there is some $\beta < \alpha$ with $\overline{x} \in M_\beta$ (this follows from the definition of a cumulative hierarchy and the fact that $\overline{x}$ is finite). Furthermore, $G(\overline{x}) \leq F(\beta) < \alpha$. The existence of y implies that $G(\overline{x}) \neq 0$, so there is some $y' \in M_{G(\overline{x})} \subseteq M_\alpha$ such that $\zeta^M(\overline{x}, y')$ holds. Since $\alpha \in C_\zeta$, this implies that $\zeta^{M_\alpha}(\overline{x}, y')$ holds as well.

Theorem 12.7. *There is no formula φ such that $Z+\varphi$ is consistent and extends ZF.*

Remark. Z here indicates ZF without Replacement; the above theorem shows that the infinite axiom schema of Replacement cannot be replaced by a finite one.

Proof. If $Z + \varphi$ extends ZF, then it derives the Reflection Principle, and in particular there is some least rank α that reflects φ and is a limit ordinal greater than ω (every club class contains arbitrarily large limit ordinals). That is,

$$Z + \varphi \vdash \exists \alpha. \lim(\alpha) \wedge \omega < \alpha \wedge \varphi^{V_\alpha} \wedge (\forall \beta < \alpha. \neg(\varphi^{V_\beta} \wedge \lim(\beta) \wedge \omega < \beta)).$$

But recall that V_α is a model of Z for every limit ordinal α greater than ω, so if γ is the least α whose existence is proven above, then

$$V_\gamma \models \exists \alpha. \lim(\alpha) \wedge \omega < \alpha \wedge \varphi^{V_\alpha}.$$

But this is a contradiction, since all the involved notions are absolute for V_γ, and so any element of V_γ satisfying the above would contradict the minimality of γ. However, to see the absoluteness of the above predicates will require some additional technical tools. To be continued. (Maybe.)

SDG

Lecture 16: The Constructible Hierarchy
March 23, 2009

13 The Constructible Hierarchy

Remark. We now return to Gödel's Constructible Hierarchy, L. Ultimately, we will show that

$$ZF \vdash ZF^L + AC^L + GCH^L$$

(where here "ZF" does not include the Axiom of Choice), thus proving the consistency of AC and GCH relative to that of ZF.

Definition 13.1. We define the constructible hierarchy L as follows:

$$\begin{aligned} L_0 &= \emptyset \\ L_{\alpha+1} &= Def(L_\alpha) \\ L_\lambda &= \bigcup_{\beta<\lambda} L_\beta, \qquad \lim(\lambda). \end{aligned}$$

Intuitively, $Def(X)$ is the collection of sets definable in $\langle X, \in\rangle$ with parameters from X. But we will take some care to nail this down more rigorously.

Remark. We assume that our formal language has variables v_i, $i \in \omega$, and the usual connectives ($=$, $\in$, $\vee$, $\neg$, $\exists$). We now define a formal coding of formulas as sets (A "Gödel-setting" scheme, if you will.)

Definition 13.2. We define a "function" $Code$ sending formulas to sets. (Note it is only a function in a metaphorical sense, not a set-theoretic one, and is used only for convenience of notation.)

$$\begin{aligned} Code(v_i = v_j) &= \langle 0, i, j\rangle \\ Code(v_i \in v_j) &= \langle 1, i, j\rangle \\ Code(\varphi \vee \psi) &= \langle 2, Code(\varphi), Code(\psi)\rangle \\ Code(\neg\varphi) &= \langle 3, Code(\varphi)\rangle \\ Code(\exists v_i.\varphi) &= \langle 4, i, Code(\varphi)\rangle\,. \end{aligned}$$

Definition 13.3. We now define a relation Fm, which relates coded formulas u to their construction depth n and a sequence s of their subformulas.

$$
\begin{aligned}
Fm(u,n,s) \triangleq\ & n \in \omega \wedge Fn(s) \wedge \mathrm{dom}(s) = n+1 \wedge s(n) = u \\
& \wedge \forall k \leq n. \\
& \Big(\exists i,j < \omega . s(k) = Code(v_i = v_j) \\
& \vee \exists i,j < \omega . s(k) = Code(v_i \in v_j) \\
& \vee \exists l,m < k . s(k) = \langle 2, s(l), s(m) \rangle \\
& \vee \exists l < k . s(k) = \langle 3, s(l) \rangle \\
& \vee \exists l < k . \exists i < \omega . s(k) = \langle 4, i, s(l) \rangle \Big)
\end{aligned}
$$

Note that $Fn(x)$ is a predicate stating that x is a function. Then we also define $Fm(u) \triangleq \exists n . \exists s . Fm(u,n,s)$.

Remark. Finally, we define a satisfaction relation on formulas with respect to a set X. The idea is that if s_i is a coding for some subformula of u, then b_i will be the set of satisfiers of s_i, that is, the set of functions that assign free variables in s_i to elements of X in such a way that s_i is satisfied.

We want to be able to bound the domain of the satisfiers in b_i, but we can't just a priori pick some arbitrary limit. However, given a coding of a formula u, we know that the rank of u (denoted $\rho(u)$ in what follows) will be big enough, since it is certainly an upper bound on the indices of the free variables occuring in u (since each is embedded as an ordinal somewhere in u).

Definition 13.4. We define the relation Sat' on sets X, coded formulas u, and sequences of sets of satisfiers b as follows:

$$
\begin{aligned}
Sat'(X,u,b) \triangleq\ & \exists n . \exists s . Fm(u,n,s) \wedge Fn(b) \wedge \mathrm{dom}(b) = n+1 \\
& \wedge \mathrm{rng}(b) \subseteq {}^{\rho(u)}X \\
& \wedge \forall k < n+1. \\
& \Big((\exists i,j < \rho(u) . s(k) = Code(v_i = v_i) \wedge \forall t \in b(k) . t(i) = t(j)) \\
& \vee (\exists i,j < \rho(u) . s(k) = Code(v_i \in v_i) \wedge \forall t \in b(k) . t(i) \in t(j)) \\
& \vee (\exists l,m < k . s(k) = \langle 2, s(l), s(m) \rangle \wedge b(k) = b(l) \cup b(m)) \\
& \vee (\exists l < k . s(k) = \langle 3, s(l) \rangle \wedge b(k) = {}^{\rho(u)}X - b(l)) \\
& \vee (\exists l < k . \exists i < \rho(u) . s(k) = \langle 4, i, s(l) \rangle \wedge b(k) = \{\, t \mid \exists a \in X . t[i \mapsto a] \in b(l) \,\}) \Big)
\end{aligned}
$$

where $t[i \mapsto a] = t - \{\langle i, t(i) \rangle\} \cup \{\langle i, a \rangle\}$.

Definition 13.5. We can now define Sat as follows:

$$Sat(X,u,t) \triangleq \exists b . \exists n \in \omega . Sat'(X,u,b) \wedge t \in b(n) \wedge \mathrm{dom}(b) = n+1.$$

Definition 13.6. We define the notions of Σ_1, Π_1, and Δ_1-T formulas as follows:

- A formula φ is Σ_1 if there is some Δ_0 formula ψ such that $\varphi = \exists x.\psi$.
- A formula φ is Π_1 if there is some Δ_0 formula ψ such that $\varphi = \forall x.\psi$.
- φ is Δ_1-T for some theory T iff there is a Σ_1 formula ψ and a Π_1 formula χ such that
$$T \vdash \forall \overline{z}(\varphi(\overline{z}) \Leftrightarrow \chi(\overline{z}) \wedge \varphi(\overline{z}) \Leftrightarrow \psi(\overline{z})).$$

Lemma 13.7. *If φ is Δ_1-T then φ is absolute for transitive models of T.*

Proof. Suppose $M \subseteq M'$ are two transitive models of T, and we have some Δ_1-T formula $\varphi(\overline{z})$. We wish to show that $\varphi^M \Leftrightarrow \varphi^{M'}$ for all $\overline{z} \in M$.

($\Rightarrow$) Suppose $\varphi^M(\overline{z})$ holds. Then since M models T, we have $(\exists x.\psi(\overline{z}, x))^M$, that is, there exists $x \in M$ such that $\psi(\overline{z}, x)^M$. But we know that M is transitive and ψ is Δ_0, so $\psi(\overline{z}, x)^{M'}$ also holds (and $x \in M'$ since $M \subseteq M'$). Therefore, $\varphi^{M'}(\overline{z})$ holds.

($\Leftarrow$) Conversely, suppose $\varphi^{M'}(\overline{z})$ holds. Then we have $(\forall x.\chi(\overline{z}, x))^{M'}$). By a similar argument, since all $x \in M'$ are also in M, and χ is Δ_0, $(\forall x.\chi(\overline{z}, x))^M$ holds, and therefore so does $\varphi^M(\overline{z})$. ∎

Remark. Now we can give the sketch of an argument that Sat is Δ_1-ZF. We first note that Sat is Σ_1 as defined (it needs to be shown that Sat' is Δ_0). But we also note that by the way we constructed Sat', if some b exists which satisfies the definition of Sat, it is unique, and so $Sat(X, u, t)$ is equivalent to

$$\forall b.(\mathrm{dom}(b) = n + 1 \wedge Sat'(X, u, b) \Rightarrow t \in b(n)),$$

which is Π_1.

Lecture 17: The Constructible Hierarchy, Part II
March 25, 2009

Definition 13.8. Following the previous lecture, we can now formally define Def.

$$\begin{aligned} Def(X) = \{\, y \subseteq X \mid & \exists \varphi. fv(\varphi) = \{v_0, \dots v_n\} \\ & \wedge \exists t.\, \mathrm{dom}(t) = \{v_0, \dots v_{n-1}\} \\ & \wedge y = \{\, a \in X \mid Sat(X, \varphi, t \cup \{\langle v_n, a\rangle\})\,\}\,\} \end{aligned}$$

Remark. Informally, we can think of this definition as

$$\begin{aligned} D(X, y) &\triangleq \exists \varphi. \exists \overline{a}. y = \{\, a \in X \mid \langle X, \in\rangle \models \varphi[\overline{a}, a]\,\} \\ Def(x) &= \{\, y \mid D(X, y)\,\}. \end{aligned}$$

Definition 13.9. A function F is Σ_1 iff the relation $F(x) = y$ is Σ_1.

Lemma 13.10. *If* $\mathrm{dom}(F)$ *is* Δ_1 *and* F *is* Σ_1*, then* F *is* Δ_1*.*

Proof. Since F is Σ_1, we may suppose that F is given by some formula $F(x, y) \triangleq \exists z. \varphi(x, y, z)$.

Now consider the formula

$$\chi(x, y) \triangleq (\mathrm{dom}\, F)(x) \wedge \forall w. (\exists z. \varphi(x, w, z)) \Rightarrow w = y.$$

We claim that χ is equivalent to F, and that it is Π_1.

First, suppose $F(x, y)$. Then there is some z for which $\varphi(x, y, z)$, and $(\mathrm{dom}\, F)(x)$ holds by definition. Now suppose there is some w for which $\exists z. \varphi(x, w, z)$ holds. Then by definition, we have $F(x, w)$. But since F is functional, $w = y$.

Conversely, suppose $\chi(x, y)$ holds. Then x is in the domain of F, so there must be some y' for which $F(x, y')$. But the second clause of $\chi(x, y)$ implies that this y' must be equal to y; hence $F(x, y)$.

To see that χ is Π_1, note that $\mathrm{dom}\, F$ is Π_1, and the $\exists$ is on the left-hand side of an implication. More concretely, supposing that $(\mathrm{dom}\, F)(x) \triangleq \forall v. \psi(v, x)$,

$$\begin{aligned} \chi(x, y) &\iff \forall v. \psi(v, x) \wedge \forall w. \neg(\exists z. \varphi(x, w, z)) \vee w = y \\ &\iff \forall v. \psi(v, x) \wedge \forall w. \forall z. \neg\varphi(x, w, z) \vee w = y \\ &\iff \forall v. \forall w. \forall z. \psi(v, x) \wedge \neg\varphi(x, w, z) \vee w = y. \end{aligned}$$

Although this seems as though it has more than one unbounded quantifier, we could rewrite it as a single universal quantification over an ordered triple (this is known as "contraction"). Hence, χ is Π_1.

Since F is Σ_1 and equivalent to a Π_1 formula, it is Δ_1. ∎

Remark. We remark that the class of Σ_1 formulas is closed under

- existential quantification,

- $\wedge$ and $\vee$ connectives, and
- bounded universal quantification.

The first two properties are obvious; the last is not.

A similar property holds for the class of Π_1 formulas.

Remark. The discussion of contraction at the end of the above proof shows that repetitions of the same unbounded quantifier are uninteresting. The above remark also shown that bounded quantifiers are not interesting. A real increase in complexity, however, comes from alternating unbounded quantifiers. Σ_2 is the class of formulas beginning with $\exists\forall$; Σ_3 formulas begin with $\exists\forall\exists$; and so on. Π_n is similar.

Lemma 13.11. *If G is Σ_1 and F is defined by transfinite recursion over G, then F is Δ_1.*

Proof. Suppose we define $F(\alpha) = G(F \restriction \alpha)$ by transfinite recursion; formally, we define

$$F(\alpha) = X \iff \exists f.\forall\beta \in \mathrm{dom}(f).f(\beta) = G(f \restriction \beta) \wedge f(\alpha) = X.$$

Note that since G is Σ_1, so is $f(\beta) = G(f \restriction \beta) \wedge f(\alpha) = X$; hence so is $F(\alpha) = X$ since the class of Σ_1 formulas is closed under bounded universal quantification and existential quantification. Also, the domain of F is the class of ordinals, which is Δ_1 (in fact, it is Δ_0), so by Lemma 13.10 F is Δ_1. ∎

Theorem 13.12. *L is Δ_1.*

Proof. L is defined by transfinite recursion over a Σ_1 function (it is left as an exercise to check that Def is Σ_1). ∎

Corollary 13.13. *L is absolute for transitive models of ZF.*

Definition 13.14. The *order* of a set X, denoted $od(X)$, is the least α such that $X \in L_{\alpha+1}$. (It is not yet clear that this is well-defined for all sets, although it turns out that it is.)

Definition 13.15. A class M is *almost universal* iff for every $X \subseteq M$, then there is some $Y \in M$ for which $X \subseteq Y$.

Lemma 13.16. *If M contains On (the class of ordinals) and is transitive and almost universal, and $(Sep)^M$ (that is, M satisfies the axiom of Separation), then $(ZF)^M$.*

Proof. Deferred to the next lecture. ∎

Lemma 13.17. *L satisfies the conditions of Lemma 13.16.*

Proof. We show each of the conditions in turn.

- L is transitive, that is, L_α is transitive for all α. Since a union of transitive sets is transitive, it suffices to show that $Def(X)$ is transitive if X is.

  Suppose X is transitive, and that $y \in Def(X)$. Thus $y \subseteq X$. We want to show that $y \subseteq Def(X)$. Suppose $z \in y$, and consider the formula $\varphi(w) = w \in z$. Then the set $\{ w \mid \langle X, \in \rangle \models \varphi(w) \} \in Def(x)$; but since X is transitive, every member of z is a member of X, so this set is equal to z, and $y \subseteq Def(X)$.

- To show that L contains On, we will in fact show the stronger statement that $L_\alpha \cap On = \alpha$, for all α. The proof is by induction on α. The base case is easily verified.

  In the limit case, $On \cap L_\lambda = On \cap \bigcup_{\beta<\lambda} L_\beta = \bigcup_{\beta<\lambda}(On \cap L_\beta) = \bigcup_{\beta<\lambda} \beta = \lambda$.

  In the successor case, suppose $On \cap L_\alpha = \alpha$. Since L is cumulative, we need only show that $\alpha \in L_{\alpha+1}$; to see this, consider the defining formula $On(\beta)$ over L_α. Since On is Δ_0, it is absolute, so it picks out exactly the elements of α.

- L is almost universal. Given $Y \subseteq L$, consider

  $$\beta = \sup\{od(x) + 1 \mid x \in Y\}.$$

  Then $Y \subseteq L_\beta \in L_{\beta+1}$.

- L satisfies Separation. Suppose $x \in L$, and consider the set

  $$s = \{ y \in x \mid \varphi^L(y) \}.$$

  We must show that s is in L also. Consider $\beta = od(x)$. By the Reflection Principle, there is some $\alpha > \beta$ such that

  $$\forall y \in L_\alpha . \varphi^L(y) \iff \varphi^{L_\alpha}(y).$$

  But since every $y \in x$ is also in L_α, this means that $s \in L_{\alpha+1}$; we may take the defining formula to be $\varphi(y) \wedge y \in x$.

Lecture 18: The Constructible Hierarchy, Part III
March 30, 2009

Proof of Lemma 13.16. We are given a transitive, almost universal class M which contains On and satisfies Sep; we wish to show that M satisfies ZF.

- Ext^M since M is transitive.
- Reg^M since M is a class.
- $Pair^M$. Suppose $x \in M$ and $y \in M$. By pairing (in the universe) there is some $z = \{x, y\} \subseteq M$. Since M is almost universal, there is some $u \in M$ such that $z \subseteq u$. Now consider the set $\{\, w \in u \mid w = x \vee w = y \,\}$. This set is in M since M satisfies Separation; but this set is precisely the pair $\{x, y\}$ in M, since $w = x \vee w = y$ is Δ_0.
- $Union^M$. Let $M(x)$. Then by the union axiom, $\exists \bigcup x. \forall z. z \in \bigcup x \Leftrightarrow \exists b \in x. z \in b$.

  Note that $y \in \bigcup x \implies y \in M$, since M is transitive; so by the almost universality of M, we conclude there is some $u \in M$ for which $\bigcup x \subseteq u$. Now consider the formula $\varphi(y) \triangleq \exists b \in x. y \in b$.

  Note that Sep^M expands to

  $$\forall x \in M. \exists y \in M. \forall z \in M. z \in y \Leftrightarrow z \in x \wedge \varphi^M(z).$$

  So we may conclude that there is some $p \in M$ such that $\forall z \in M. z \in p \Leftrightarrow z \in u \wedge \varphi^M(z)$, that is,

  $$p = \{\, z \in u \mid \varphi^M(z) \,\}.$$

  We want to show the union axiom relativized to M, that is, $\exists q \in M. \forall z \in M. z \in q \Leftrightarrow \varphi^M(z)$. We claim that p witnesses this formula. The $(\Rightarrow)$ direction holds by definition of p. The $(\Leftarrow)$ direction holds since φ is Δ_0, so $\varphi^M(z)$ implies $\varphi(z)$ (since $z \in M$) and $\varphi(z)$ states that $z \in \bigcup x$; and $\bigcup x \subseteq u$.
- $Powerset^M$. Let $M(x)$. Then by the power set axiom, $\mathcal{P}(x)$ exists in the universe. Note that this may *not* be the power set of x in M, since M does not necessarily contain all subsets of x. We want to show that

  $$v = \{\, w \in \mathcal{P}(x) \mid M(w) \,\}$$

  is in M. Since M is almost universal, there is some $u \in M$ for which $v \subseteq u$; then by comprehension in M we may form the set $\{\, z \in u \mid z \subseteq x \,\}$; this set is precisely v ($\subseteq$ is Δ_0).
- $Infinity^M$. We stipulated that $On \subseteq M$, so in particular we have $\omega \in M$, and ω is absolute.

- *Replacement*^{M}. Suppose $\varphi(x, y)$ is a functional relation in M, that is, $\forall x \in M. \exists! y \in M. \wedge \varphi^M(x, y)$. We wish to show

$$\forall w \in M. \exists u \in M. \forall x \in w. \exists y \in u. \varphi^M(x, y).$$

  This is the relativization to M of a weak form of the axiom of replacement. It shows that u contains the image of w under φ; we can use separation to construct the exact image of w under φ.

  Let $w \in M$; the φ-image of w exists in the universe, call it v. Then by almost universality of M, there is some $u' \in M$ for which $v \subseteq u'$; then we are done. ∎

Corollary 13.18. *ZF^L.*

Definition 13.19. A model M of ZF is an *inner model* iff M is a transitive class containing On.

Remark. We have seen previously that there is a Δ_1-ZF relation C such that $C(\alpha, x)$ iff $x = L_\alpha$. Hence $C(\alpha, x)$ is absolute for inner models of ZF.

Lemma 13.20. *If M is an inner model of ZF, then $L^M = L$. (Where $L^M = \{ y \mid (\exists \alpha, x.\, C(\alpha, x) \wedge y \in x)^M \}$.)*

Proof. ??? ∎

Corollary 13.21. *$ZF \vdash (V = L)^L$.*

Proof. $(V = L)^L = (V^L = L^L) = (L = L)$. ∎

Corollary 13.22. *L is the smallest inner model of ZF.*

Proof. Any inner model M contains $L^M = L$. ∎

Remark. Recall that we are in the middle of trying to prove

$$ZF \vdash ZF^L + AC^L + GCH^L,$$

by showing that

$$ZF + \text{“}V = L\text{”} \vdash AC + GCH$$

and

$$ZF \vdash ZF^L + (V = L)^L.$$

We have now shown the second part; it remains only to show that AC and GCH hold in $ZF +$ “$V = L$”.

Theorem 13.23. *$ZF + (V = L) \vdash AC$.*

Proof. There is a definable relation $<_L$ which is a global well-ordering of L (this is bizarre). Define $<_{L,\alpha}$ inductively as follows.

- $<_{L,0}$ is the empty relation.

- At limit stages, we of course take the union of all previous stages.
- Now we define $<_{L,\alpha+1}$ in terms of $<_{L,\alpha}$. Note that every $x \in L_{\alpha+1}$ is a subset of L_α defined in terms of some $n \in \omega$, some $\overline{y} \in L_\alpha^n$, and some first-order formula φ. We can order formulas using a Gödel numbering. We can also order tuples lexicographically, so given an ordering of L_α, we can order elements of L_α^n. We now order $L_{\alpha+1}$ in the obvious way: for each $x \in L_{\alpha+1}$, choose (in some canonical order) the least n, least formula φ, and least tuple that define it. Also, we stipulate that everything at stage α comes before everything first arising at stage $\alpha + 1$.

We then take $x <_L y$ to mean that there exists some α for which $x <_{L,\alpha} y$.

Hence every set in L has a well-ordering, so AC holds. (But moreover, the entire universe is well-ordered! This gives an intuitive reason to believe that $V = L$ is not really true in a Platonic sense.) ∎

Lecture 19: The Constructible Hierarchy, Part IV
April 1, 2009

Remark. We now proceed to prove the generalized continuum hypothesis under the assumption that $V = L$.

Lemma 13.24. *For every infinite ordinal α,* $\mathrm{card}(L_\alpha) = \mathrm{card}(\alpha)$.

Proof. First, we note that $L_\omega = V_\omega$, and $\mathrm{card}(V_\omega) = \mathrm{card}(\omega) = \omega$. Also, it is clear that $\mathrm{card}(L_\alpha) \geq \mathrm{card}(\alpha)$ since $\alpha \subseteq L_\alpha$.

In the successor case, we want to show that $\mathrm{card}(L_{\alpha+1}) = \mathrm{card}(Def(L_\alpha)) = \mathrm{card}(\alpha+1) = \mathrm{card}(\alpha)$. This amounts to showing that Def preserves cardinality. But every element of $Def(L_\alpha)$ is a formula together with some finite number of witnesses from L_α; hence its size is at most

$$\aleph_0 \times \sum_{n\in\omega} (\mathrm{card}(L_\alpha))^n = \mathrm{card}(L_\alpha). \qquad \square$$

Definition 13.25. $o(M)$ is the least γ for which $\gamma \notin M$. For transitive M, $o(M) = \{\gamma \mid \gamma \in M\}$.

Remark. Recall that the GCH says that $2^\kappa = \kappa^+$ for all infinite κ. To show that it holds in L, we must show that every subset of L_κ occurs at some level prior to L_{κ^+}. If we can show that $od(x) < \kappa^+$ for every $x \leq \kappa$, then $2^\kappa \leq \kappa^+$ (we already know that $2^\kappa \geq \kappa^+$ by Cantor's Theorem). In particular, we will show that for every $x \subseteq L_\alpha$, $od(x) < |\alpha|^+$.

Recall that $\alpha \mapsto L_\alpha$ is Δ_1-ZF. So there is some sentence θ for which $\alpha \mapsto L_\alpha$ is Δ_1-θ, that is, θ proves the equivalence of the Σ_1 and Π_1 forms of $\alpha \mapsto L_\alpha$. Given this, we can prove the following lemma.

Lemma 13.26. *There is a sentence θ such that* $\mathrm{ZF} + (V = L) \vdash \theta$ *and for every transitive M,*

$$M \models \theta \implies \exists\alpha.\, \lim(\alpha) \wedge M = L_\alpha.$$

Proof. Let ψ be the function $\alpha \mapsto L_\alpha$. Then $\psi(\alpha, x)$ is absolute for transitive models of a finite fragment θ' of ZF. Then let

$$\theta = \theta' \wedge (V = L).$$

If $M \models \theta$, the claim is that $M = L_\alpha$ for some $\lim(\alpha)$.

In particular, we claim that $M = L_{o(M)}$.

- Since $\alpha \mapsto \alpha + 1$ is absolute for M, $o(M)$ must be a limit.
- $L_\alpha \subseteq M$. Since $\lim(\alpha)$, $L_\alpha = \bigcup_{\beta<\alpha} L_\beta$, and $\beta \in M$ for all $\beta < \alpha$. $\psi(\beta, x)$ is absolute for M, so $L_\beta \in M$ for all $\beta < \alpha$. Hence, $\bigcup_{\beta<\alpha} L_\beta \subseteq M$ by transitivity of M.

- $M \subseteq L_\alpha$. Note that $M \models V = L$. For $\beta < \alpha$, $(L_\beta)^M = L_\beta$; hence $M \subseteq \bigcup_{\beta<\alpha} L_\beta$.

∎

Theorem 13.27. *For every x, α, if $L(x)$ and $x \subseteq L_\alpha$ then there is some $\beta < |\alpha|^+$ with $x \in L_\beta$.*

Remark. We first remark that this theorem implies the GCH; note that if $x \subseteq \kappa$ then $x \subseteq L_\kappa$. This theorem says that every subsset of L_α gets constructed at some stage prior to $|\alpha|^+$; hence the *set* of all such subsets must occur at stage $|\alpha|^+$.

Proof. Observe that θ is a conseqnece of $V = L$. Since θ is a single sentence, we can apply the Reflection Principle.

Suppose $x \subseteq L_\alpha$ and $L(x)$; hence there is some δ with $x \in L_\delta$. Pick $\beta > \delta$, $\beta > \alpha$, $\lim(\beta)$ from the club class of ordinals reflecting θ in L. Hence $x \in L_\beta$, and we note that $L_\alpha \subseteq L_\beta$.

Since AC holds in L, by the Löwenheim-Skolem theorem there is some $N \preceq L_\beta$ such that $L_\alpha \cup \{x\} \subseteq N$ and $|N| = \text{card}(\alpha)$; we also note that $N \models \theta$ since $N \preceq L_\beta$. Also, observe that $L_\alpha \cup \{x\}$ is transitive, since $x \subseteq L_\alpha$. (However, N might not be transitive.)

But N *is* extensional and well-founded, so by the Mostowski collapsing theorem, it is isomorphic to a unique transitive set M, and the isomorphism preserves $L_\alpha \cup \{x\}$ (the Mostowski isomorphism is the identity on any transitive sets).

Hence $M \models \theta$ since it is isomorphic to N. So $M = L_\gamma$, $\lim(\gamma)$, with $\alpha < \gamma < |\alpha|^+$ ($\alpha < \gamma$ since $L_\alpha \subseteq L_\gamma$; $\gamma < |\alpha|^+$ since M has cardinality α). ∎

Lecture 20: Independence of CH, part I
April 6, 2009

14 Independence of CH

Remark. We will now spend the next few lectures proving the independence of CH from ZFC, as shown by Cohen in 1963 by the (in)famous "method of forcing." In particular, we will show that $Con(ZFC) \implies Con(ZFC+\neg CH)$, since we have already shown (via the Constructible Hierarchy) that $Con(ZFC) \implies Con(ZFC + CF)$.

The general idea is that we will start with a countable transitive model M of ZFC (hereafter, "countable transitive model of ZFC" will be abbreviated "ctm"). (We note that for every finite $T \subseteq ZFC$, there is some countable transitive model of T, via the Reflection principle, Löwenheim-Skolem, and Mostowski.)

Then we will construct a set $G \notin M$ and a ctm $M[G]$ such that

- $G \in M[G]$,
- $o(M) = o(M[G])$,
- $M \subseteq M[G]$, and
- $M[G]$ is the least such extension of M.

Then note that $M[G] \models ZFC + V \neq L$ (since $L^M = L^{M[G]}$).

Now suppose $ZFC + \neg CH \vdash 0 = 1$. Then by compactness there is a finite T such that $T + \neg CH \vdash 0 = 1$. Then we will show that if M is a ctm for $T \subseteq T'$, then $M[G]$ is a ctm for $T' \cup \neg CH$. (T' is T plus the finite amount of stuff we need to throw in to make the various proofs involved go through).

Remark. Let M be a ctm. We will now consider partial orders $\langle \mathbb{P}, \leq, 1\rangle \in M$ with a maximal element 1. Note that in what follows, $\mathbb{P}$ will always refer to an arbitrary such partial order with maximal element. First, let's look at some examples, which will come in handy later and serve to motivate some of the definitions to come.

Let $FP(X, Y)$ be the set of finite partial functions from X to Y. This forms a poset with reverse extension as the ordering (that is, $p \leq q \iff q \subseteq p$) and the empty function as the maximal element. The idea is that partial functions specify constraints on some sort of model, and $p \leq q$ holds exactly when all models that satisfy p also satisfy q (but p may be more restrictive than q, so fewer models may satisfy it).

A particular example of this sort of structure is $FP(\omega, 2)$, the set of finite partial functions from ω to 2. We can think of elements of this partial order as specifying conditions on a binary real number (the values of some places are specified, and some are not).

Definition 14.1. Let $p, q \in \mathbb{P}$. Then p is *compatible* with q, denoted $p \top q$, if there exists $r \in \mathbb{P}$ such that $r \leq p$ and $r \leq q$.

p is *incompatible* with q, denoted $p \perp q$, iff they are not compatible.

Remark. Compatibility of p and q is just a formal way of saying that p and q don't conflict; that is, they do not represent contradictory constraints.

Definition 14.2. A set $X \subseteq \mathbb{P}$ is *upward closed* iff for every $p \in X$ and every $q \in \mathbb{P}$, if $p \leq q$ then $q \in X$.

Definition 14.3. $G \subseteq \mathbb{P}$ is a *filter* iff

- Any two elements of G are compatible, and
- G is upward closed.

Definition 14.4. $D \subseteq \mathbb{P}$ is *dense in* $\mathbb{P}$ iff for every $p \in \mathbb{P}$, there exists some $q \in D$ for which $q \leq p$.

Remark. As an example, the set $D_n = \{\, p \mid n \in \mathrm{dom}(p) \,\}$ is dense in $FP(\omega, 2)$ for all n.

Definition 14.5. $G \subseteq \mathbb{P}$ is $\mathbb{P}$-*generic over* M iff for every $\mathbb{P}$-dense $D \in M$,

- $G \cap D \neq \emptyset$, and
- G is a filter.

Lemma 14.6. *For every ctm M, $\mathbb{P} \in M$ and $p \in \mathbb{P}$, there is some $G \subseteq \mathbb{P}$ with $p \in G$ such that G is $\mathbb{P}$-generic over M.*

Proof. Since M is countable, we may enumerate the dense sets in M; call them $D^1, D^2, D^3, \ldots$.

Now let $p_0 = p$, and for each $i + 1$ pick $p_{i+1} \in D^{i+1}$ such that $p_{i+1} \leq p_i$ (such a p_{i+1} must exist since D^{i+1} is dense).

Let G be the upward closure of $\{p_0, p_1, \ldots\}$. Then G is a filter by transitivity of $\leq$, and its intersection with every dense set in M is non-empty by construction; hence G is a $\mathbb{P}$-generic set over M which contains p. SDG

Remark. Consider again the example of $FP(\omega, 2)$. We already noted that the family of sets D_n defined above are dense. Note also that $D_n \in M$ for any ctm M, which we can show by various tedious absoluteness arguments. (We must also note that $FP(\omega, 2) \in M$, but this can also be seen by various straightforward absoluteness arguments.)

By Lemma 14.6 we know that there is some set G which is $FP(\omega, 2)$-generic over M. Now consider $f = \bigcup G$. Since G is a filter, f is a partial function $\omega \to 2$ (G does not contain any incompatible elements, so taking its union does not result in any disagreements, and f is therefore functional).

Moreover, since $D_n \in M$ for all n and G is $FP(\omega, 2)$-generic, we must have $n \in \mathrm{dom}(f)$ for all n (G must contain some element of D_n for every n). Hence f is actually a total function $\omega \to 2$.

Two big questions immediately spring to mind: is $G \in M$? And is $f \in M$?

Lemma 14.7. *Suppose every element of $\mathbb{P}$ has incompatible extensions; that is, for every $p \in \mathbb{P}$, there exist $q, r \in \mathbb{P}$ such that $q \leq p$, $r \leq p$, and $q \perp r$. Then if G is $\mathbb{P}$-generic over M, $G \notin M$.*

Proof. Suppose otherwise, that is, $G \in M$. Then $\mathbb{P} - G \in M$. We claim that $\mathbb{P} - G$ is dense: every $p \in \mathbb{P}$ has incompatible extensions, which can't both be in G, so there is at least one $q \leq p$ with $q \in \mathbb{P} - G$. But then, by definition of a $\mathbb{P}$-generic set, we have $G \cap (\mathbb{P} - G) \neq \emptyset$, which is absurd. ∎

Remark. For example, $FP(\omega, 2)$ clearly has the property described in the above lemma; given some finite partial function p, pick some $n \notin \mathrm{dom}(p)$, and define q and r to be extensions of p which send n to 0 and 1, respectively. So the G described in the previous remark is not an element of M. Moreover $f = \bigcup G \notin M$ as well; if it were, we would be able to construct G in M.

We can now restate our goal: given a ctm M, some partial order $\mathbb{P} \in M$, and some G which is $\mathbb{P}$-generic over M, we want to show that there is a ctm $M[G]$ satisfying the conditions in the opening remarks.

Remark. Consider again $FP(X, Y) \in M$, the poset of finite partial functions from X to Y. (We assume that $X \in M$ and $Y \in M$.) Assume further that X is infinite, and $Y \neq \emptyset$.

We know that there exists a G which is $FP(X, Y)$-generic over M. Again, let $f = \bigcup G$. By an argument similar to that before, f is a partial function from X to Y since G is a filter. Also, for every $a \in X$ we may define $D_a = \{\, p \mid a \in \mathrm{dom}(p) \,\}$ which is dense, so again f is in fact a total function.

Moreover, we may also define $D^b = \{\, p \mid b \in \mathrm{rng}(p) \,\}$; these sets are also dense since X is infinite (we can always pick an unused element of the domain to map to the chosen element of the range). Thus, we conclude that f is surjective.

For example, we can look at $FP(\omega, (\aleph_\omega)^M)$. Following the above construction, we get a surjective function that "collapses" $\aleph_\omega$ in $M[G]$. More on this in the next lecture.

Lecture 21: Independence of CH, part II
April 8, 2009

Theorem 14.8. *$M[G] \models ZFC + \neg CH$.*

Remark. Of course, this proof is modulo a number of lemmas that we haven't proved yet (in fact, we haven't even yet defined $M[G]$!). But we are now at a point to give the high-level structure of the proof, and fill in the details later.

Proof. Given a ctm M, consider $FP(\kappa \times \omega, 2)$ where $(\kappa > \aleph_1)^M$ and $Card^M(\kappa)$, and let G be $FP(\kappa \times \omega, 2)$-generic over M. Then as noted previously, $F = \bigcup G$ is a total, surjective function $\kappa \times \omega \to 2$.

(Note that $\kappa \in M$ is a cardinal *in* M, that is, $Card^M(\kappa)$. It may not be a cardinal in the universe! In fact, since M is countable and transitive, κ definitely isn't a cardinal in the universe unless $\kappa = \omega$.)

Now define a "curried" version of F,

$$f_\alpha(n) = F(\langle \alpha, n \rangle),$$

and for any $\alpha \neq \beta$, define

$$D_{\alpha\beta} = \{\, p \in \mathbb{P} \mid \exists n. \big(\, \langle \alpha, n \rangle \in \mathrm{dom}(p) \wedge \langle \beta, n \rangle \in \mathrm{dom}(p) \wedge p(\langle \alpha, n \rangle) \neq p(\langle \beta, n \rangle)\big) \,\}.$$

That is, $D_{\alpha\beta}$ is the set of partial functions which disagree at $\langle \alpha, n \rangle$ and $\langle \beta, n \rangle$ for some n. Note that if $G \cap D_{\alpha\beta} \neq \emptyset$, then $f_\alpha \neq f_\beta$, since there will be some n for which f_α and f_β disagree.

However, $D_{\alpha\beta}$ is dense for all distinct $\alpha, \beta < \kappa$: given any $p \in \mathbb{P}$, we may pick some $n \notin \mathrm{dom}(p)$ and construct $q \in D_{\alpha\beta}$ to be p extended with $q(\langle \alpha, n \rangle) = 0$ and $q(\langle \beta, n \rangle) = 1$. It is also not hard to see that $D_{\alpha\beta} \in M$. But G has nonempty intersection with every dense set in M; therefore, f_α and f_β are distinct for every distinct α and β.

Thus, we have a κ-sized collection of binary valued functions on ω, and hence $2^\omega > \kappa$: we may pick $\kappa = \aleph_2$ to observe that the CH is not true in $M[G]$. ∎

Remark. There is one teensy worry with the last sentence of the above proof—what if $M[G]$ collapses cardinals? That is, although κ is a certain cardinal in M, we may worry that it gets collapsed to something smaller in $M[G]$, so that the above argument says nothing in particular about the CH in $M[G]$. We will see that this is not the case, but proving it will take considerable effort.

Lemma 14.9 ($M[G]$ preserves cardinals)**.** *If $\kappa > \omega$ and $\kappa < o(M)$ and $M \models Card(\kappa)$, then $M[G] \models Card(\kappa)$.*

Remark. This is enough to show not only that κ is still a cardinal in $M[G]$, but that it is a cardinal just as big in $M[G]$ as in M (that is, it can't be collapsed to a smaller cardinal). This follows from the fact that the notion of being greater than some other cardinal is absolute.

To prove this lemma, we'll first need a number of definitions and sublemmas.

Definition 14.10. $X \subseteq \mathbb{P}$ is an *antichain* iff $p \perp q$ for every distinct $p, q \in X$.

Definition 14.11. We say that $\mathbb{P}$ has the *ccc* (embarrassingly, this stands for "countable chain condition") iff every antichain $X \subseteq \mathbb{P}$ is countable.

Definition 14.12. Z is a *quasi-disjoint* collection of sets iff there exists an a such that $u \cap v = a$ for every pair of distinct elements $u, v \in Z$.

Lemma 14.13. *Every uncountable collection of finite sets has an uncountable, quasi-disjoint subset.*

Proof. Let S be an uncountable collection of finite sets. Without loss of generality, we may assume that every $u \in S$ has cardinality n, for some $n \in \omega$ (note that for some i,

$$S_i = \{\, u \in S \mid |u| = i \,\}$$

is uncountable).

The proof is by induction on n. The base case, $n = 1$, is easy; we may just take $a = \emptyset$.

If $n > 1$, there are two cases to consider.

- First, suppose that for some e, there are uncountably many $u \in S$ with $e \in u$. Let T denote the set of all such u, and let

  $$T^- = \{\, u - \{e\} \mid u \in T \,\}.$$

  This is an uncountable collection of sets of size $n - 1$, so by the inductive hypothesis, there is an uncountable, quasi-disjoint subset of T^-, call it T^*. But we may then form the set $Q = \{\, u \cup \{e\} \mid u \in T^* \,\}$, which is an uncountable subset of T which is quasi-disjoint—if the common intersection of the elements of T^* is a, the common intersection of the elements of Q is $a \cup \{e\}$.

- Now suppose that there is no element e which occurs in uncountably many $u \in S$. For each $e \in \bigcup S$, let T_e denote the set of all $u \in S$ which contain e. We now recursively construct a sequence of pairwise disjoint $u_\alpha \in S$ for $\alpha < \aleph_1$ as follows.

  Pick $u_0 \in S$ arbitrarily. Now for each $0\gamma < \aleph_1$, consider the set

  $$T_\gamma = \{\, T_e \mid e \in u_\beta \text{ for some } \beta < \gamma \,\}.$$

  T_γ is a countable union of countable sets (there are countably many u_β, each of which is finite, and by hypothesis each T_e is countable), and hence countable. Therefore $S - T_\gamma$ is nonempty and we may arbitrarily pick $u_\gamma \in S - T_\gamma$. ☒

Lecture 22: Independence of CH, part III
April 13, 2009

Lemma 14.14. *If Y is countable, then $FP(X,Y)$ has the ccc.*

Proof. Suppose Y is countable and consider any uncountable set of finite partial functions

$$P = \{ p_\alpha \mid \alpha < \aleph_1 \} \subseteq FP(X,Y).$$

We wish to show that P is not an antichain.

Let $Z = \mathrm{dom}[P]$. By Lemma 14.13, there is some $Z' \subseteq Z$ which is uncountable and quasi-disjoint. Let d be the common intersection of the elements of Z', and consider the set of functions ${}^dY$. This set is countable since Y is countable and d is finite.

For $p, q \in FP(X,Y)$, define $p \sim q$ iff $p \restriction d = q \restriction d$, and $P' = \{ p_\alpha \mid \mathrm{dom}(p_\alpha) \in Z' \}$. Consider $P'/\sim$: each equivalence class is represented by some function $d \to Y$, so there are countably many equivalence classes. However, P' is uncountable, so there must be some uncountable equivalence class, call it B. But any two $p, q \in B$ are compatible, since they agree on d, the intersection of their domains. Hence P is not an antichain: in fact, it must contain *uncountably many* compatible elements! ∎

Lemma 14.15 (Approximation Lemma)**.** *If $(\mathbb{P}$ has the ccc$)^M$, M is a ctm, $X, Y \in M$ and $f : X \to Y \in M[G]$, then there is an $F : X \to \mathcal{P}(Y) \in M$ such that for every $a \in X$, $f(a) \in F(a)$ and $(F(a)$ is countable$)^M$.*

Remark. This lemma essentially says that given any function $f \in M[G]$, we may "approximate" it in M, even though f itself may not be an element of M. We defer the proof of this lemma to the remainder of the semester.

Lemma 14.16. *If $(\mathbb{P}$ has the ccc$)^M$ and M is a ctm, then $Card^M(\kappa)$ implies $Card^{M[G]}(\kappa)$.*

Remark. Note that $Card(\kappa)$ denotes "κ is a cardinal"; not to be confused with $\mathrm{card}(\kappa)$, the cardinality of κ. We also note that this lemma is only interesting for uncountable κ, since finite cardinals and ω are absolute; we don't have to worry about those getting collapsed in $M[G]$.

Proof. Suppose, by way of contradiction, that $Card^M(\kappa)$ but there is some infinite $\beta < \kappa$ and some $f \in M[G]$ with $f : \beta \xrightarrow[\text{onto}]{} \kappa$.

By Lemma 14.15, there is some $F : \beta \to \mathcal{P}(\kappa) \in M$ for which $\bigcup \mathrm{rng}(F) = \kappa$. But now $(\mathrm{card}(\kappa) = \kappa = \mathrm{card}(\bigcup \mathrm{rng}(F)) \leq \mathrm{card}(\beta) \times \aleph_0 = \mathrm{card}(\beta) < \kappa)^M$, a contradiction. ∎

Definition 14.17. τ is a $\mathbb{P}$-name iff τ is a relation and for every $\langle \sigma, p \rangle \in \tau$, σ is a $\mathbb{P}$-name and $p \in \mathbb{P}$.

Remark. This definition might seem circular, but we can formalize it by induction on the transitive closure of τ.

Definition 14.18. Suppose τ is a $\mathbb{P}$-name and $G \subseteq \mathbb{P}$. Then define

$$\mathrm{val}(\tau, G) = \{\, \mathrm{val}(\sigma, G) \mid \exists p \in G.\, \langle \sigma, p \rangle \in \tau \,\}.$$

Definition 14.19. $V^{\mathbb{P}}$ denotes the class of all $\mathbb{P}$-names. $M^{\mathbb{P}}$ denotes $M \cap V^{\mathbb{P}}$, which is equal to $(V^{\mathbb{P}})^M$ because of some lemma about recursion and absoluteness.

Remark. Let's look quickly at a few examples.

- Of course, $\emptyset \in V^{\mathbb{P}}$ trivially; $\mathrm{val}(\emptyset, G) = \emptyset$ for all G.
- Also, consider $\tau = \{\langle \emptyset, p \rangle\} \in V^{\mathbb{P}}$. We have

$$\mathrm{val}(\tau, G) = \begin{cases} \{\emptyset\} & p \in G \\ \emptyset & \text{otherwise.} \end{cases}$$

- $\rho = \{\langle \emptyset, 1_{\mathbb{P}} \rangle\}$ is also a valid $\mathbb{P}$-name; $\mathrm{val}(\rho, G) = \{\emptyset\}$ for all filters G.
- We may generalize this to

$$\dot{x} = \{\, \langle \dot{y}, 1_{\mathbb{P}} \rangle \mid y \in x \,\}.$$

  We can consider $\dot{x}$ to be a "canonical name" for x: $\mathrm{val}(\dot{x}, G) = x$ for every filter G.

Definition 14.20. Given a ctm M, $\mathbb{P} \in M$, and a G which is $\mathbb{P}$-generic over M, define

$$M[G] = \{\, \mathrm{val}(\tau, G) \mid \tau \in M^{\mathbb{P}} \,\}.$$

Remark. By the above remark concerning canonical names, we observe that $M \subseteq M[G]$.

Lecture 23: Independence of CH, part IV
April 15, 2009

Remark. In the previous lecture, we defined the generic extension $M[G]$ of any ctm M with respect to a set G which is $\mathbb{P}$-generic over M. Today, we will begin to verify that it has the required properties. In particular:

- $M \subseteq M[G]$. (We showed this in the previous lecture.)
- $G \in M[G]$.
- $M[G]$ is transitive.
- $o(M) = o(M[G])$.
- $M[G]$ is a ctm.
- $M[G]$ is the least extension of M with these properties.

Lemma 14.21. *$G \in M[G]$.*

Proof. Consider the set

$$\Delta = \{ \langle \dot{p}, p \rangle \mid p \in \mathbb{P} \}.$$

We have already seen that $\dot{x} \in M$ whenever $x \in M$, so $\Delta \in M$ by pairing and replacement (M is a ctm). Also, Δ is clearly a $\mathbb{P}$-name. But $\mathrm{val}(\Delta, G) = G$, so we conclude that $G \in M[G]$. ∎

Lemma 14.22. *$M[G]$ is the least extension of M with the required properties.*

Proof. Suppose there is some ctm N such that $M \subseteq N$ and $G \in N$. $M^{\mathbb{P}} \subseteq N$ since $M \subseteq N$, so $\mathrm{val}(\tau, G) \in N$ for all $\tau \in M^{\mathbb{P}}$ (val is definable in $M[G]$, and absolute since it is defined by recursion). Therefore, $M[G] \subseteq N$. ∎

Remark. From now on we will use the abbreviation τ_G in place of $\mathrm{val}(\tau, G)$.

Lemma 14.23. *$M[G]$ is transitive.*

Proof. Suppose $x \in M[G]$ and $y \in x$. By definition of $M[G]$, there is some $\tau \in M^{\mathbb{P}}$ for which $x = \tau_G$. Expanding out the definition of τ_G, we have

$$x = \tau_G = \{ \sigma_G \mid \exists p \in G.\, \langle \sigma, p \rangle \in \tau \}.$$

Therefore $y = \sigma_G$ for some $\sigma \in V^{\mathbb{P}}$, but since M is transitive, $\sigma \in M$ as well (since τ is). Hence $y \in M[G]$. ∎

Lemma 14.24. *$o(M) = o(M[G])$.*

Proof. $o(M) \leq o(M[G])$ follows directly from the fact that $M \subseteq M[G]$.

To show that $o(M[G]) \leq o(M)$, we show that $\text{rank}(\tau_G) \leq \text{rank}(\tau)$, by structural induction on τ. If $\tau = \emptyset$, then $\text{rank}(\tau_G) = \text{rank}(\emptyset) = 0$.

In the inductive case,

$$\begin{aligned}
\text{rank}(\tau_G) &= \text{rank}(\{\, \sigma_G \mid \exists p \in G.\, \langle \sigma, p\rangle \in \tau \,\}) \\
&\leq \text{rank}(\{\, \sigma_G \mid \langle \sigma, p\rangle \in \tau \,\}) \\
&\leq \text{rank}(\{\, \sigma \mid \langle \sigma, p\rangle \in \tau \,\}) \qquad \text{(IH)} \\
&\leq \text{rank}(\{\, \langle \sigma, p\rangle \mid \langle \sigma, p\rangle \in \tau \,\}) \\
&= \text{rank}(\tau).
\end{aligned}$$

Now we note that if $\alpha \in M[G]$, then there is some $\tau \in M$ for which $\tau_G = \alpha$, and $\alpha = \text{rank}(\alpha) \leq \text{rank}(\tau) = \beta$, and that $\text{rank}(\tau) \in M$ whenever $\tau \in M$. (??) ∎

Remark. It remains to show that $M[G]$ is a ctm; but before we do that, we talk about the method of forcing, and use it to prove the Approximation Lemma (Lemma 14.15).

Definition 14.25. Let M be a ctm and $\mathbb{P} \in M$ a poset with a maximal element. Suppose $\varphi(x_1, \ldots, x_n)$ is some formula and $\tau_1, \ldots, \tau_n \in M^{\mathbb{P}}$. Then p *forces* $\varphi(\tau_1, \ldots, \tau_n)$, written

$$p \Vdash_{M,\mathbb{P}} \varphi(\tau_1, \ldots, \tau_n),$$

iff for every G which is a $\mathbb{P}$-generic extension over M with $p \in G$,

$$M[G] \models \varphi(\tau_{1G}, \ldots, \tau_{nG}).$$

Remark. Often M and $\mathbb{P}$ will be clear from the context and we omit the subscripts on $\Vdash$.

Remark. We now state two essential (and somewhat surprising) results about forcing; their proofs will be put off until later.

Theorem 14.26 (Truth)**.** *$M[G] \models \varphi(\tau_{1G}, \ldots, \tau_{nG})$ if and only if there is some $p \in G$ for which $p \Vdash \varphi(\tau_1, \ldots, \tau_n)$.*

Theorem 14.27 (Definability)**.** *For every $\varphi(x_1, \ldots, x_n)$, there is a formula denoted*

$$p \Vdash^* \varphi(x_1, \ldots, x_n)$$

such that for all $\tau_1, \ldots, \tau_n$, $p \Vdash \varphi(\tau_1, \ldots, \tau_n)$ if and only if $M \models (p \Vdash^* \varphi(\tau_1, \ldots, \tau_n))$.

Remark. In other words, the notion of forcing is definable within M itself. This is rather surprising, since the definition of forcing quantifies over all generic extensions, which are not elements of M!

Lemma 14.28 (Preservation of forcing)**.** *For all formulas φ and $s, t \in \mathbb{P}$, if $s \leq t$ and $t \Vdash \varphi$, then $s \Vdash \varphi$.*

Proof. Suppose $s \nVdash \varphi$—that is, there is some G $\mathbb{P}$-generic over M with $s \in G$ and $M[G] \not\models \varphi$. But since G is a filter, it is upward closed; hence $s \in G$ implies $t \in G$, which is a contradiction since $t \Vdash \varphi$. ∎

Remark. We now return to prove the Approximation Lemma (Lemma 14.15).

Proof of Lemma 14.15. Let $\tau \in M^{\mathbb{P}}$ such that $\tau_G = f$. By Theorem 14.26 (Truth), there is some $p \in G$ such that $p \Vdash \tau : \dot{x} \to \dot{y}$.

Now, for each $a \in X$, define

$$F(a) = \{\, b \mid \exists q \leq p.\ q \Vdash \tau(\dot{a}) = \dot{b} \,\}.$$

Then by definability of forcing in M (Theorem 14.27) and the fact that M is a ctm, we have that $F \in M$.

Now suppose $f(a) = b$; we wish to show that $b \in F(a)$. Since $f(a) = b$, in particular we have that $M[G] \models \tau_G(a) = b$. Hence, by Truth, there is some $r \in G$ such that $r \Vdash \tau(\dot{a}) = \dot{b}$. Since G is a filter and $p, r \in G$, there is some $q \in G$ for which $q \leq p$ and $q \leq r$. By Lemma 14.28, $q \Vdash \tau(\dot{a}) = \dot{b}$. But then $b \in F(a)$ by definition.

Finally, we show that $F(a)$ is countable in M for every $a \in X$. Since M is a ctm, it satisfies AC, so there is a choice function $g : F(a) \to G$ such that $g(b) \leq p$ and $g(b) \Vdash \tau(\dot{a}) = \dot{b}$ for each $b \in F(a)$; that is, for each b, g picks a witness of the fact that $b \in F(a)$. (We note that for each b, the set of q which witness $b \in F(a)$ is in M by definability of forcing and the fact that M is a ctm.)

We claim that for any two distinct $b, b' \in F(a)$, $g(b) \perp g(b')$. (Note that this also implies that g is injective.) To see this, suppose $b \neq b'$ and $g(b) \top g(b')$. Then since G is a filter, there exists some r for which $r \leq g(b)$ and $r \leq g(b')$. But then by preservation of forcing,

$$\begin{aligned} &r \Vdash \tau : \dot{x} \to \dot{y} \text{ (since } r \leq g(b) \leq p), \\ &r \Vdash \tau(\dot{a}) = \dot{b}, \text{ and} \\ &r \Vdash \tau(\dot{a}) = \dot{b'}, \end{aligned}$$

which is a contradiction since we assumed that $b \neq b'$.

Therefore, $g[F(a)]$ is an antichain, and hence countable in M since $\mathbb{P}$ has the ccc in M by assumption. Therefore, since g is injective, $F(a)$ is countable in M. ∎

Remark. We now know, by Lemma 14.16, that any extension of a ctm M defined with respect to a $FP(\aleph_2 \times \omega, 2)$-generic set doesn't collapse cardinals.

We also note the general shape of the preceding proof: we went from some combinatorial property of a partial order $\mathbb{P}$ (here, the ccc property of $FP(X, Y)$) to a property of $\mathbb{P}$-generic extensions of a ctm M. This is typical of forcing arguments, although in general the combinatorial proerties may be much more complicated, and the proofs correspondingly more difficult.

Lecture 24: Independence of CH, part V
April 20, 2009

Lemma 14.29. *$M[G]$ is a ctm of ZFC.*

Proof. We show that $M[G]$ satisfies each axiom of ZFC.

- Extensionality. Follows easily from transitivity of $M[G]$.
- Regularity. Trivial.
- Pairing. Let $x, y \in M[G]$; then there exist $\tau, \sigma \in M^{\mathbb{P}}$ with $\tau_G = x$ and $\sigma_G = y$. Now consider the set

  $$\delta = \{\langle \tau, 1_{\mathbb{P}} \rangle, \langle \sigma, 1_{\mathbb{P}} \rangle\}.$$

  It is easy to see that $\delta_G = \{\tau_G, \sigma_G\} = \{x, y\}$. But note that $\delta \in M^{\mathbb{P}}$: it is a $\mathbb{P}$-name by construction, and is in M since M is a ctm.
- Union. Suppose $a \in M[G]$. We wish to show that there is some $b \in M[G]$ which contains $\bigcup a$ as a subset (we can then appeal to Separation in $M[G]$, which we will show later).

  Since $a \in M[G]$, there is some $\tau \in M^{\mathbb{P}}$ with $\tau_G = a$. Let $\pi = \bigcup \mathrm{dom}(\tau)$; this is a set which contains the $\mathbb{P}$-names of all elements of τ_G (and possibly some extra ones whose corresponding conditions are not in G). $\pi \in M$ since M is a ctm; $\pi \in V^{\mathbb{P}}$ by construction ($\mathrm{dom}(\tau)$ is a set of $\mathbb{P}$-names, so $\bigcup \mathrm{dom}(\tau)$ is a subset of $V^{\mathbb{P}} \times \mathbb{P}$). Hence $\pi \in M^{\mathbb{P}}$, so $\pi_G \in M[G]$.

  We claim that $\bigcup a \subseteq \pi_G$. To see this, let $c \in a$; then $c = \sigma_G$ for some $\sigma \in \mathrm{dom}(\tau)$. Therefore $\sigma \subseteq \pi$, so $\sigma_G \subseteq \pi_G$.
- Separation. Let $\sigma \in M^{\mathbb{P}}$ and let φ be a formula (it may have multiple parameters, but we omit them in the following proof), and define

  $$c = \{\, a \in \sigma_G \mid M[G] \models \varphi[a] \,\}.$$

  We wish to show that $c \in M[G]$, which we will do by finding a suitable $\mathbb{P}$-name for c.

  We claim that a suitable $\mathbb{P}$-name is

  $$\rho = \{\, \langle \pi, p \rangle \in \mathrm{dom}(\sigma) \times \mathbb{P} \mid p \Vdash \pi \in \sigma \wedge \varphi(\pi) \,\}.$$

  We first note that $\rho \in M$ by separation in M and definability of $\Vdash$ (Theorem 14.27); ρ is clearly a $\mathbb{P}$-name by construction. Now we must show that $\rho_G = c$.

  - ($\rho_G \subseteq c$). Suppose $x \in \rho_G$, so there is some $\langle \pi, p \rangle \in \rho$ such that $x = \pi_G$ and $p \Vdash \pi \in \sigma \wedge \varphi(\pi)$ and $p \in G$. Then by definition of forcing, $\pi_G \in \sigma_G$ and $M[G] \models \varphi[\pi_G]$. Hence $x = \pi_G \in c$ by definition of c.

– $(c \subseteq \rho_G)$. Suppose $a \in c$, that is, $a \in \sigma_G$ and $M[G] \models \varphi[a]$. Then there is some $\pi \in M^{\mathbb{P}}$ such that $\pi_G = a$. So by Truth (Theorem 14.26) we may pick $p \in G$ such that $p \Vdash \pi \in \sigma \wedge \varphi(\pi)$. Then $\langle \pi, p \rangle \in \rho$, so $a = \pi_G \in \rho_G$.

- Replacement. At this point, we introduce the axiom schema of Collection:

$$\forall x.\exists y.\forall z \in x.(\exists w.\varphi(z,w) \Rightarrow \exists w \in y.\varphi(z,w)).$$

Intuitively, this states that we can collect elements in the image of any set x under any partial relation φ into a set y (which may also contain other stuff). This implies the axiom schema of Replacement: we may take φ to be a functional relation, and then given a set y witnessing Collection, we may use Separation to yield a set which is exactly the image $\varphi[x]$.

It turns out that Collection is also a theorem of ZF, via the reflection principle.

Now suppose we have some $x = \sigma_G$; we wish to exhibit a ρ for which

$$M[G] \models \forall z \in \sigma_G.(\exists w.\varphi(z,w) \Rightarrow \exists w \in \rho_G.\varphi(z,w)). \tag{2}$$

Let $S \in M$ such that

$$\begin{aligned} M \models \forall \pi \in \mathrm{dom}(\sigma).\forall p \in \mathbb{P}.(\exists \mu.M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi,\mu) \\ \Rightarrow (\exists \mu \in S).p \Vdash \varphi(\pi,\mu)). \end{aligned}$$

It is not *a priori* clear that such an S exists. If $M^{\mathbb{P}}$ were a set, we could just take $S = M^{\mathbb{P}}$, but $M^{\mathbb{P}}$ may be a proper class. However, such an S does exist, which we can show as follows (note that in the following, all our reasoning is taking place *inside* M). By Reflection in M, there is a closed unbounded class of ordinals α which simultaneously reflect the two formulae

$$\exists \mu.M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi,\mu)$$

and

$$M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi,\mu),$$

that is,

$$\begin{aligned} \forall \pi \in \mathrm{dom}(\sigma).\forall p \in \mathbb{P}.\big(\exists \mu.M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi,\mu) \\ \Leftrightarrow [\exists \mu.M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi,\mu)]^{V_\alpha}\big), \end{aligned} \tag{3}$$

and

$$\begin{aligned} \forall \pi \in \mathrm{dom}(\sigma).\forall p \in \mathbb{P}.\forall \mu.\big(M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi,\mu) \\ \Leftrightarrow [M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi,\mu)]^{V_\alpha}\big). \end{aligned} \tag{4}$$

So, we may pick such an α large enough so that $\mathrm{dom}(\sigma) \in V_\alpha$ and $\mathbb{P} \in V_\alpha$.

We then let $S = M^{\mathbb{P}} \cap V_\alpha$, and claim that S has the required property. Given some $\pi \in \mathrm{dom}(\sigma)$ and $p \in \mathbb{P}$, suppose there exists some $\mu \in M^{\mathbb{P}}$ for which $p \Vdash \varphi(\pi, \mu)$. Then by equation (3) there is some $\mu \in V^\alpha$ which satisfies $[M^{\mathbb{P}}(\mu) \wedge p \Vdash \varphi(\pi, \mu)]^{V_\alpha}$; but then by equation (4) μ also satisfies this condition in the universe, so $\mu \in S$ and $p \Vdash \varphi(\pi, \mu)$, exactly the required property of S.

Now let $\rho = S \times \{1_{\mathbb{P}}\}$, so $\rho_G = \{\, \mu_G \mid \mu \in S \,\}$ (since G is a filter). Now we must show that ρ satisfies equation (2).

To this end, let $z \in \sigma_G$ and $\varphi^{M[G]}(z, w)$ for some $w \in M[G]$. We must find some $w' \in \rho_G$ for which $\varphi^{M[G]}(z, w')$.

Since $z \in \sigma_G$, $z = \pi_G$ for some $\pi \in \mathrm{dom}(\sigma)$. We know that $M[G] \models \exists w.\varphi(\pi_G, w)$, so there must be some μ for which $M[G] \models \varphi(\pi_G, \mu_G)$. Then by Truth there is some $p \in G$ such that $p \Vdash \varphi(\pi, \mu)$. Then by the property of S, there is some $\mu' \in S$ such that $p \Vdash \varphi(\pi, \mu')$, and $\mu'_G \in \rho_G$. ∎

Remark. We are not quite done; in the next lecture we will cover Powerset and Choice. But now, a small digression about the axiom schema of Collection.

Definition 14.30. *Kripke-Platek set theory* is the axiomatic system with Extensionality, Regularity, Pairing, Union, and all Δ_0 instances of Separation and Collection.

Remark. It is easy to see that $V_\omega \models KP$, since it models ZF − Infinity. KP + Infinity is a nice system, too.

Definition 14.31. An ordinal α is *admissible* iff $L_\alpha \models KP$.

Remark. Admissible ordinals "are those which support a nice notion of computability."

Definition 14.32. $R \subseteq \omega \times \omega$ is *recursive* iff c_R, the characteristic function of R, is Turing-computable. An ordinal α is recursive iff it is the order type of some recursive $R \subseteq \omega \times \omega$.

Definition 14.33. ω_1^{CK}, the *Church-Kleene ordinal*, is the least non-recursive ordinal.

$(\omega_1^{CK})^f$ is the least non-$(\text{recursive})^f$ ordinal, where $f \in \omega \to 2$ and $(\text{recursive})^f$ means Turing-computable given an f-oracle.

Theorem 14.34. *If α is a countable ordinal greater than ω, then α is admissible iff $\alpha = (\omega_1^{CK})^f$ for some $f \in \omega \to 2$.*

Remark. The proof is omitted.

We note that ω_1^{CK} is, in fact, the set of all recursive ordinals, so in particular it must be countable (since there are countably many Turing machines).

Lecture 25: Independence of CH, part VI
April 22, 2009

Remark. We now return to finish the proof that $M[G]$ is a ctm.

Proof.
- Powerset. Let $\sigma_G \in M[G]$. We wish to construct some $\rho \in M^{\mathbb{P}}$ such that
$$\forall x. x \subseteq \sigma_G \Rightarrow x \in \rho_G.$$
This suffices, because once we have obtained a covering of the power set in this manner, we can use Separation to cut out the exact power set.

  To this end, let
$$S = \{\, \tau \in M^{\mathbb{P}} \mid \mathrm{dom}(\tau) \subseteq \mathrm{dom}(\sigma) \,\}.$$
We note that $S \in M$, since it is equal to $[\mathcal{P}(\mathrm{dom}(\sigma) \times \mathbb{P})]^M$, and $\mathcal{P}(\mathrm{dom}(\sigma) \times \mathbb{P})$ exists in M since it is a ctm.

  Now let $\rho = S \times \{1_{\mathbb{P}}\}$. We claim that this is the desired ρ. To see this, suppose $\mu \in M^{\mathbb{P}}$ and $\mu_G \subseteq \sigma_G$; we must show that $\mu_G \in \rho_G$. Let
$$\tau = \{\, \langle \pi, p \rangle \mid \pi \in \mathrm{dom}(\sigma) \wedge p \Vdash \pi \in \mu \,\}.$$
We note that $\tau \in M$ by definability of forcing; also, τ has the form of a $\mathbb{P}$-name, so $\tau \in M^{\mathbb{P}}$. Then by definition of S, it is easy to see that $\tau \in S$. Therefore, $\tau_G \in \rho_G$.

  To complete the proof, we claim that $\tau_G = \mu_G$.

  - $(\mu_G \subseteq \tau_G)$. Let $y \in \mu_G$. Since $\mu_G \subseteq \sigma_G$, there must be some $\pi \in \mathrm{dom}(\sigma)$ for which $y = \pi_G \in \sigma_G$. Therefore, by Truth, there is some $p \in G$ for which $p \Vdash \pi \in \mu$. So $\langle \pi, p \rangle \in \tau$ by definition, and hence $y = \pi_G \in \tau_G$ (since $p \in G$).
  - $(\tau_G \subseteq \mu_G)$. Suppose $y \in \tau_G$. Then $y = \pi_G$ for some π with $\langle \pi, p \rangle \in \tau$, $p \in G$, and $p \Vdash \pi \in \mu$. So, by definition of forcing, $y = \pi_G \in \mu_G$.

- Choice. We first give the following alternate formulation of the well-ordering principle:
$$\forall x. \exists f. \exists \alpha \in Ord. \, \mathrm{dom}(f) = \alpha \wedge x \subseteq \mathrm{rng}\, f.$$
Some thought should show that this is equivalent to the familiar version of the well-ordering principle; given a set x, if we have a function f postulated by the above axiom, then we can use f to construct a well-ordering of x: put the elements of x in order according to the least β such that $f(\beta)$ yields them.

  Fix $x = \sigma_G$. Since M satisfies Choice, there is some well-ordering π of the elements of $\mathrm{dom}(\sigma)$:
$$\mathrm{dom}(\sigma) = \{\, \pi_\gamma \mid \gamma < \alpha \,\}$$

where $Ord(\alpha)$ and the function $\pi_{(-)} \in M$. π is a well-ordering of the domain of σ, which consists of names of elements of x (possibly plus some extra names). It is not hard to see that we can use a well-ordering of the names of elements of x to construct a well-ordering of x, as follows.

Let $\tau = \{\, \dot{\langle}\dot{\gamma}, \pi_\gamma\dot{\rangle} \mid \gamma < \alpha \,\} \times \{1_{\mathbb{P}}\}$, where $\dot{\langle}x, y\dot{\rangle}$ denotes the name for which $\dot{\langle}x, y\dot{\rangle}_G = \langle x_G, y_G\rangle$. $\tau \in M^{\mathbb{P}}$ since M is a ctm. Moreover,

$$\tau_G = \{\, \langle \gamma, (\pi_\gamma)_G\rangle \mid \gamma < \alpha \,\}.$$

So τ_G is a function with domain α and $\sigma_G \subseteq \operatorname{rng} \tau_G$, as desired. ∎

Remark. Hence, $M[G]$ is a ctm; putting this result together with previous results, we have now shown (modulo the proofs of Truth and Definability) that there is a G for which

$$M[G] \models ZFC + \neg CH,$$

and therefore that CH is formally independent of ZFC!

15 Ramsey cardinals

Remark. And now, for something completely different! We will now attempt to show that

$$ZFC + Q \vdash V \neq L,$$

where Q is a large cardinal axiom. But first, Ramsey's Theorem!

Definition 15.1. For any set κ, we introduce the notation

$$[\kappa]^n = \{\, x \subseteq \kappa \mid \operatorname{card}(x) = n \,\},$$

that is, the collection of n-element subsets of κ. While this definition makes sense for any cardinal n, we will only use it for $n \in \omega$.

Definition 15.2. For any cardinals κ and λ, we define the relation

$$\kappa \to (\lambda)^n_\mu$$

to hold iff for every function $f : [\kappa]^n \to \mu$, there exists a set x such that

- $x \subseteq \kappa$,
- $\operatorname{card}(x) = \lambda$, and
- $f \restriction [x]^n$ is constant.

Remark. $f : [\kappa]^n \to \mu$ can be seen as a labeling of the n-element subsets of κ, using labels from μ. For example, if $n = 2$, such an f can be thought of as an edge coloring of the complete graph on κ nodes, using μ colors. If $\kappa \to (\lambda)^2_\mu$ holds, it means that we can find a subset of nodes of size λ which induces a monochromatically colored complete subgraph.

Theorem 15.3 (Ramsey's Theorem)**.** $\omega \to (\omega)^n_m$ *for all* $n, m \in \omega$.

Remark. This seems somewhat surprising! But it is true. In the finite case, it is famously true that for any $l \in \omega$, there exists some $k \in \omega$ such that $k \to (l)^2_2$, but the growth rate of the smallest such k with respect to l is astronomical (and unknown). Note famous quote by Erdős regarding this function and hostile aliens.

Proof. We will only prove the case for $\mu = n = 2$; it should be straightforward to see how to generalize the proof.

Let $f : [\omega]^2 \to \{0, 1\}$. We wish to construct a set $X \subseteq \omega$ of size ω for which $f \restriction [X]^2$ is constant. We mutually construct three sequences a_i, b_i, and X_i as follows:

$$\begin{aligned} X_0 &= \omega \\ a_0 &= 0 \\ X_{i+1} &= \{\, n \in X_i \mid f(\{a_i, n\}) = b_i \,\} && b_i \in \{0, 1\} \text{ such that } X_{i+1} \text{ is infinite} \\ a_{i+1} &= \text{least } n \in X_{i+1} \text{ such that } n > a_i \end{aligned}$$

Note that we can always pick an appropriate b_i by an infinite version of the pigeonhole principle.

Again by the pigeonhole principle, either infinitely many $b_i = 0$, or infinitely many $b_i = 1$. So we may choose $X = \{\, a_i \mid b_i = b \,\}$, for whichever value of b makes X infinite (note that all the a_i are distinct since we chose them to form an increasing sequence).

We claim that $f \restriction [X]^2$ is constantly b. Let $a_i, a_j \in X$, and suppose, without loss of generality, that $j < k$. We know that $a_k \in X_k$; but since the X_i form a decreasing chain, $a_k \in X_{j+1}$ as well. But then by definition, $f(\{a_j, a_k\}) = b_j = b$. ∎

Lecture 26: Ramsey cardinals
April 27, 2009

Definition 15.4. κ is *weakly compact* iff κ is uncountable and $\kappa \to (\kappa)^2_2$.

Lemma 15.5. *If κ is weakly compact, then $\kappa \to (\kappa)^2_\mu$ for every $\mu < \kappa$.*

Proof. The proof is a problem on the final exam. ∎

Lemma 15.6. *If κ is weakly compact, then κ is strongly inaccessible.*

Proof. We must show that κ is regular, and that it is a strong limit.

- κ is regular. Suppose otherwise; then let $\lambda < \kappa$ and $\{ \gamma_\alpha \mid \alpha < \lambda \} \subseteq \kappa$ an increasing sequence with $\sup\{ \gamma_\alpha \mid \alpha < \lambda \} = \kappa$. Without loss of generality, assume $\gamma_0 = 0$.

  We note that γ naturally induces a partition of κ into λ many segments. Now, define

  $$f(\{\delta, \zeta\}) = \begin{cases} 0 & \exists \alpha \geq 0. \delta, \zeta \in [\gamma_\alpha, \gamma_{\alpha+1}), \\ 1 & \text{otherwise.} \end{cases}$$

  f induces a 2-partition on $[\kappa]^2$; hence, since κ is weakly compact, there must be some set $Y \subseteq \kappa$ of cardinality κ where f is constant on $[Y]^2$.

  Since f is constant on $[Y]^2$, there are two cases to consider. First, we could have $Y \subseteq [\gamma_\alpha, \gamma_{\alpha+1})$ for some α; but this is a contradiction since $|[\gamma_\alpha, \gamma_{\alpha+1})| \leq \gamma_{\alpha+1} < \kappa$, and $|Y| = \kappa$. Alternatively, we could have $\text{card}(Y \cap [\gamma_\alpha, \gamma_{\alpha+1})) \leq 1$ for all α. But then $|Y| \leq \lambda < \kappa$, another contradiction.

- κ is a strong limit. Suppose otherwise, that is, there is some $\lambda < \kappa$ with $\kappa \leq 2^\lambda$. Then there exists some injective function $g \xrightarrow{1\text{-}1} {}^\lambda 2$. (Recall that ${}^\lambda 2$ is the set of functions from λ to 2.) Now use g to define a partition $f : [\kappa]^2 \to \lambda$ as follows:

  $$f(\{\alpha, \beta\}) = \text{the least } \gamma \text{ for which } g_\alpha(\gamma) \neq g_\beta(\gamma).$$

  We note that f is total since g is injective.

  However, it is impossible to find a homogenous set of size three under this partition, much less size κ.

∎

Definition 15.7. κ s a *Ramsey cardinal* iff $\kappa \to (\kappa)^{<\omega}_2$.

Lemma 15.8. *If κ is a Ramsey cardinal, then $\kappa \to (\kappa)^{<\omega}_\mu$ for all $\mu < \kappa$.*

Proof. This is also a problem on the final exam. ∎

Lemma 15.9. *Suppose κ is a Ramsey cardinal, and $\langle D, N, E\rangle$ is a directed graph with a binary coloring on the nodes (in particular, D is the set of nodes, $N \subseteq D$ is the set of nodes which are red, and $E \subseteq D \times D$ is the set of edges) such that $|D| = \kappa$ and $|N| = \lambda < \kappa$. Then there is some $\langle D', N', E'\rangle \preceq \langle D, N, E\rangle$ such that $|D'| = \kappa$ and $|N'| = \aleph_0$.*

Proof. Fix a collection of Skolem functions for $\langle D, N, E\rangle$, and let $h(X)$ denote the Skolem hull of X in $\langle D, N, E\rangle$ for $X \subseteq D$.

For every finite $C \subseteq D$, let

$$f(C) = N_C \text{ where } h(C) = \langle D_C, N_C, E_C\rangle .$$

Since $N_C \subseteq N$ for each $C \subseteq D$, we note that $f : [D]^{<\omega} \to \mathcal{P}(N)$, so it is a partition of finite subsets of D into at most 2^λ classes.

Since κ is a Ramsey cardinal, it is weakly compact, and hence strongly inaccessible by Lemma 15.6. Therefore $2^\lambda < \kappa$, and again since κ is a Ramsey cardinal, we conclude by Lemma 15.8 that there is some set $Y \subseteq D$ of cardinality κ for which f is constant on $[Y]^n$ for all $n \in \omega$. For each n, let $X_n = f(C)$ for $|C| = n$.

Note that X_n is countable for all n, since $f(C) = N_C \subseteq D_C$, and the Skolem hull of a finite set is countable.

Now let $\langle D', N', E'\rangle = h(Y)$. We claim that $h(Y) = \bigcup_{C \subseteq_{\text{fin}} Y} h(C)$, where $A \subseteq_{\text{fin}} B$ denotes that A is a finite subset of B: a proof that $y \in h(Y)$ consists of a finite tree with elements of Y at the leaves and Skolem functions at the internal nodes, so for each y we may choose C to be the set containing all the leaves.

$h(Y) \preceq \langle D, N, E\rangle$ by construction; $N' = \bigcup_{n\in\omega} X_n$, which is countable; and taking the Skolem hull preserves cardinality, so $|D'| = |Y| = \kappa$. ∎