The Continuum Hypothesis

Susan, Summer 2018

1 The Dominating Function Question

1.1 Basic Cardinality Facts

This class lists basic facts about cardinality as a prerequisite. Just so everyone's on the same page, here's what you need to know:

Two sets A and B have the same **cardinality**, or are **equinumerous** if there exists a bijection between the two sets. Sometimes it's hard to find a bijection, but there's a result called the **Cantor-Bernstein** or **Schroeder-Bernstein** theorem[1], which says that if there exists an injection from A to B, and another injection from B to A, then a bijection exists.

A set is **countably infinite** if it is the same size as $\mathbb{N}$. Sets that are countably infinite include $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$.

A set is **the size of the continuum** if it is the same size as $\mathbb{R}$. Sets that are continuum-sized include $\mathbb{R}$, $[0,1]$, $(0,1)$, and $\mathscr{P}(\mathbb{N})$.

The powerset $\mathscr{P}(A)$ of a set A always has a larger cardinaltiy than A. We have $|\mathscr{P}(\mathbb{N})| = |\mathbb{R}|$, which gives us $|\mathbb{N}| < |\mathbb{R}|$, but are there any cardinalities in between the two? This question was open for about a hundred years before it was proven to be independent of ZFC. In this class, we'll be exploring set theoretic universes in which intermediate cardinalities exist.

Good to go? Right—onward!

1.2 Dominating Functions

Let f and g be functions from $\mathbb{N}$ to $\mathbb{N}$. We say g **dominates** f and write $g >_* f$ if there exists $n \in \mathbb{N}$ such that for any $m > n$, we have $g(m) > f(m)$. That is, the function g is *eventually bigger* than the function f.

[1]It gets called both, but it's okay, because as far as I can tell the result is actually due entirely to Bernstein.

Suppose we have a set of functions $\mathscr{F} = \{f_n \mid n \in \mathbb{N}\}$ from $\mathbb{N}$ to $\mathbb{N}$. We ask the following questions:

Warmup Question: Does there necessarily exist a function g such that $f_n <_* g$ for all $n \in \mathbb{N}$?

Answer: Yes! Take $g(n) = \max_{i<n}\{f_i(n)\} + 1$.

Slightly Harder Question: What if we take $\mathscr{F} = \{f_r : r \in \mathbb{R}\}$?

Answer: Not necessarily. $\mathbb{R}$ is equinumerous with the set of functions from $\mathbb{N}$ to $\mathbb{N}$, so $\mathscr{F}$ could be the set of all functions. That'd be pretty hard to dominate.

Our Question For Today: What if $\mathscr{F} = \{f_\alpha : \alpha \in \omega_1\}$?

If the continuum hypothesis is true, we've already answered this question. But what if ω_1 is strictly smaller than 2^ω? Turns out, this question is independent of ZFC+$\neg$CH.[2] Our goal for the next two days is to show that, assuming Martin's Axiom, we can construct a function g which dominates every $f \in \mathscr{F}$.

1.3 Recycling the Previous Proof

The proof that we used in the countable case clearly doesn't work here, but there are pieces we can recycle if we think carefully about what, exactly is going on in the proof. This is a constructive proof by recursion on the natural numbers. All constructions like this follow a particular pattern:

- We want to construct an object X that behaves in a particular way with respect to every natural number n.
- In the n'th step, we guarantee that X behaves nicely with respect to n.

Our construction was fairly compact, so it's a little difficult to see exactly how these steps fit. Let's try to break it down:

- We want to construct a function g which dominates every function f_n.
- On the n'th step, we do two things:
  - We choose a value for $g(n)$.

[2]Though the proof of this fact is a little beyond the scope of this class.

– We *promise* that from now on, whenever we pick a value for $g(k)$, it will be larger than $f_n(k)$.

Choosing a value here was the obvious step—we have to choose values to construct a function, after all. But the important step—the thing that really makes this construction work—is the promises that we're making as we go! That's the step where we guarantee that g is going to dominate f_n. For each f_n, we know that if we take any $m > n$, we will have $g(m) > f_n(m)$, because in the n'th step we promised that we would make that happen.

This sort of recursive construction is great for performing a countable number of tasks in a countable number of steps. Here the "tasks" are making sure that g dominates each one of the functions f_n. The countability is nice, because it allows us to proceed linearly. At each step, we add one additional piece of information about our function g (Namely, the value of $g(n)$), and when we're all done, we've constructed a complete function $g : \mathbb{N} \to \mathbb{N}$ that does exactly what we want it to do.

Unfortunately, when we lose countability, we lose the ability to proceed through each step in the construction in order. So if we can't use a linear order, what's the next best thing?

1.4 A Partial Order!

So! We want to build a function that dominates uncountably many functions f_α, but we can't proceed linearly. We know that over the course of the construction, we will be doing two things: choosing values, and making promises. This means that if we press pause midway through the process, we're going to have:

- A finite piece of a function $\phi : \{1, 2, \ldots, n\} \to \mathbb{N}$.
- A finite set of promises we've made, represented by a subset $\mathscr{F}_0$ of $\mathscr{F}$, the set of functions we intend to dominate.

Whenever we extend our partial function ϕ to get a bigger piece of g, we keep our promises by making sure that the new values $g(n)$ are larger than the corresponding $f_\alpha(n)$ for all $f_\alpha \in \mathscr{F}_0$.

For example, suppose we have an ordered pair $(\phi, \mathscr{F}_0)$, with

$$\begin{array}{rccc} \phi: & 0 & \mapsto & 5 \\ & 1 & \mapsto & 3 \\ & 2 & \mapsto & 4 \end{array}$$

and with $\mathscr{F}_0 = \{f, g, h\}$, such that $f(n) = n$, $g(n) = n^n$, and $h(n) = 100$. We think of this ordered pair as a freeze-frame in the construction of our function g. At this moment, we've chosen values at 0, 1, and 2. When we choose a value for 3, it needs to be greater that $f(3) = 3$, $g(3) = 27$, and $h(3) = 100$. So we can choose any number greater than 100.

We can arrange these freeze-frames into a poset $\mathbb{P}_{\mathscr{F}}$, with ordering relation given by $(\phi, \mathscr{F}_0) \geq (\psi, \mathscr{F}_1)$ if and only if

(i) ψ is an extension of ϕ.

(ii) $\mathscr{F}_0 \subseteq \mathscr{F}_1$.

(iii) For any $f \in \mathscr{F}_0$ and for any $m \in (\mathrm{dom}(\psi) \setminus \mathrm{dom}(\phi))$, we have $\psi(m) > f(m)$.

Roughly speaking, $(\phi, \mathscr{F}_0) \geq (\psi, \mathscr{F}_1)$ if $(\psi, \mathscr{F}_1)$ is a valid extension of $(\phi, \mathscr{F}_0)$.[3] The first condition ensures that in moving from $(\phi, \mathscr{F}_0)$ to $(\psi, \mathscr{F}_1)$, we haven't changed any of the values that we had already defined at stage $(\phi, \mathscr{F}_0)$. The second condition ensures that we haven't removed any of the promises we'd made at stage $(\phi, \mathscr{F}_0)$.[4] The third condition ensures that as we extend ϕ to obtain ψ, we honor all of the promes that were made in $(\phi, \mathscr{F}_0)$. We say that $(\psi, \mathscr{F}_1)$ is a **strengthening** of $(\phi, \mathscr{F}_0)$.

If $(\phi, \mathscr{F}_0) \geq (\psi, \mathscr{F}_1)$ and $(\varphi, \mathscr{F}_2) \geq (\psi, \mathscr{F}_1)$, then we call $(\psi, \mathscr{F}_1)$ a **common strengthening** of $(\phi, \mathscr{F}_0)$ and $(\varphi, \mathscr{F}_2)$. In this case, we say that $(\phi, \mathscr{F}_0)$ and $(\varphi, \mathscr{F}_2)$ are **compatible**, since they could both be freeze-frames in the construction of the same function. Two elements p and q that are not compatible are called **incompatible**, and we write $p \perp q$.

[3] This may seem somewhat backwards, since the "larger" ordered pair actually gives us a smaller piece of the function. Try thinking about it like this: the ordered pair represents the collection of all possible functions that could result from this freeze-frame appearing in the construction. Extending the function or making more promises makes the number of possible functions smaller.

[4] No takebacks!

1.5 We Found A Dominating Function!

Just kidding, we totally didn't. But let's pretend that we did. Assume that there exists a function g such that $g >_* f$ for every $f \in \mathscr{F}$. Consider the set $G \subseteq \mathbb{P}_{\mathscr{F}}$ such that for every $(\phi, \mathscr{F}_0) \in G$,

(i) g is an extension of ϕ.

(ii) For any $f \in \mathscr{F}_0$ and for any $m \notin \text{dom}(\phi)$, we have $g(m) > f(m)$.

That is to say, G consists of all ordered pairs representing freeze-frames that could appear in the construction of the function g. Notice that G has several nice properties:

(a) If p and q are both in G, then there exists $r \in G$ with $r \leq p$ and $r \leq q$. That is, all elements of G are compatible.

(b) For all p and q in $\mathbb{P}_{\mathscr{F}}$ such that $q \geq p \in G$, we have q in G. We say that the set G is "closed upwards" in $\mathbb{P}_{\mathscr{F}}$.

Any subset X of a poset $\mathbb{P}$ that satisfies conditions (a) and (b) is called a **filter**. Tomorrow we will discuss a couple of additional important properties of G, and talk about how we can use such a set to build a dominating function for $\mathscr{F}$.

1.6 Homework!

The primary homework for this class will be to review the concepts from the class and make sure you're ready to dive in for the next day. Most of the homework problems in this class are exercises designed to make this a bit easier. Starred problems represent exercises that prove results that we will not prove rigorously in class.

1. Suppose $\mathscr{F}$ is the set of constant functions and $g(n) = 2n$.
   (a) Show that $g >_* f$ for all $f \in \mathscr{F}$.
   (b) What does the filter G from section 1.5 look like? find necessary and sufficient conditions for an element $(\phi, \mathscr{F}_0)$ of the poset $\mathbb{P}_{\mathscr{F}}$ to be in G.

2. A **partially ordered set** or a **poset** is a set $\mathbb{P}$, together with a relation $\leq$ satisfying:
   (i) **Reflexivity:** If $p \in \mathbb{P}$, then $p \leq p$.
   (ii) **Antisymmmetry:** If $p, q \in \mathbb{P}$ satisfy $p \leq q$ and $q \leq p$, then $p = q$.
   (iii) **Transitivity:** If $p, q, r \in \mathbb{P}$ satisfy $p \leq q$ and $q \leq r$, then $p \leq r$.
   Prove that $\mathbb{P}_{\mathscr{F}}$, together with the strengthening relation, forms a poset.

3. Prove that the set G defined today in class is a filter. That is...
   (a) Prove that any two elements of G have a common strengthening.
   (b) Prove that if $(\phi, \mathscr{F}_0) \in G$, and $(\psi, \mathscr{F}_1) \geq (\phi, \mathscr{F}_0)$, then $(\psi, \mathscr{F}_1) \in G$.

4. Given below are four different elements of $\mathbb{P}_{\mathscr{F}}$. Decide which pairs are compatible, and which are incompatible. If possible, find a common strengthening.

$$\phi_1 : \begin{cases} 0 \to 1 \\ 1 \to 4 \\ 2 \to 6 \end{cases}, \qquad \begin{array}{c} \mathscr{F}_1 = \{a, b\} \\ a(n) = 2 \\ b(n) = n^2 \end{array}$$

$$\phi_2 : \begin{cases} 0 \to 1 \end{cases}, \qquad \begin{array}{c} \mathscr{F}_2 = \{c\} \\ c(n) = 3n \end{array}$$

$$\phi_3 : \begin{cases} 0 \to 0 \\ 1 \to 4 \end{cases}, \qquad \begin{array}{c} \mathscr{F}_3 = \{a, d\} \\ a(n) = 2 \\ d(n) = n + 2 \end{array}$$

$$\phi_4 : \begin{cases} 0 \to 47 \end{cases}, \qquad \mathscr{F}_4 = \emptyset$$

5. Let $\mathbb{P}$ be a poset, and let $p \in \mathbb{P}$. Is there necessarily a filter in $\mathbb{P}$ containing p? Either describe such a filter, or explain why it cannot exist.

6. A subset D of a poset $\mathbb{P}$ is called **dense** if for any $p \in \mathbb{P}$, there exists $q \leq p$ such that $q \in D$. Show that the following sets are dense in $\mathbb{P}_{\mathscr{F}}$:

   (a) The set of $(\phi, \mathscr{F}_0)$ such that $1,000 \in \mathrm{dom}(\phi)$.

   (b) The set of $(\phi, \mathscr{F}_0)$ such that for a particular $f \in \mathscr{F}$, we have $f \in \mathscr{F}_0$.

2 Martin's Axiom

2.1 The Filter G

Last time we were trying to show that given a set $\mathscr{F} = \{f_\alpha : \alpha \in \omega_1\}$ of functions from $\mathbb{N}$ to $\mathbb{N}$, we can find a function $g : \mathbb{N} \to \mathbb{N}$ that dominates all of them. So far, we've shown that *if* such a function exists, then we can find a subset $G \subseteq \mathbb{P}_{\mathscr{F}}$ such that for every $(\phi, \mathscr{F}_0) \in G$,

(i) g is an extension of ϕ.

(ii) For any $f \in \mathscr{F}$ and for any $m \notin \text{dom}(\phi)$, we have $g(m) > f(m)$.

This set G represents all elements of $\mathbb{P}_{\mathscr{F}}$ which *could* be used to build the function g. We also observed that G has these two properties:

(a) If p and q are both in G, then there exists $r \in G$ with $r \leq p$ and $r \leq q$. That is, all elements of G are compatible.

(b) For all p and q in $\mathbb{P}_{\mathscr{F}}$ such that $q \geq p \in G$, we have q in G. We say that the set G is "closed upwards" in $\mathbb{P}_{\mathscr{F}}$.

A subset of a poset in which any two elements are compatible, and which is closed upwards is called a *filter*. We also have two additional properties:

(c) For each $n \in \mathbb{N}$, there exists $(\phi, \mathscr{F}_0) \in G$ such that $n \in \text{dom}(\phi)$.

(d) For each $f \in \mathscr{F}$, there exists $(\phi, \mathscr{F}_0) \in G$ such that $f \in \mathscr{F}_0$.

So let's recap! So far we have the following:

Theorem:

There exists a function g which dominates f_α for all $\alpha \in \omega_1$.

$\Rightarrow$

There exists a filter G satisfying properties (c) and (d).

2.2 Actually, Make That An Iff

Okay, that was fun. But now, instead of assuming our goal-function g exists, let's instead assume instead that there exists a subset G of $\mathbb{P}_{\mathscr{F}}$ satisfying properties (a), (b), (c), and (d). that is, there exists a filter G that intersects with every D_n and with every D_f.

Claim: G allows us to build a function g which will dominate every $f \in \mathscr{F}$.

Proof. We define g to be equal to

$$\bigcup \{\phi \mid \exists\ \mathscr{F}_0 \subseteq \mathscr{F} \text{ such that } (\phi, \mathscr{F}_0) \in G\}\ ^5$$

We need to show that this gives us a well defined function g on all of $\mathbb{N}$ that dominates f for every $f \in \mathscr{F}$.

Let's start by showing that g is well-defined. Suppose $(\phi, \mathscr{F}_0)$ and $(\psi, \mathscr{F}_1)$ are both in G, and that both ϕ and ψ are defined on n. We want to show that $\phi(n) = \psi(n)$. We know that $(\phi, \mathscr{F}_0)$ and $(\psi, \mathscr{F}_1)$ have a common strengthening: call it $(\Phi, \mathscr{F}_2)$. Then $\phi(n) = \Phi(n)$ and $\psi(n) = \Phi(n)$, so we must have $\phi(n) = \psi(n)$.

Now we'll show that g is defined on all of $\mathbb{N}$. For any $n \in \mathbb{N}$, we have $G \cap D_n \neq \emptyset$. So there exists $(\phi_n, \mathscr{F}_n) \in G$ such that ϕ_n is defined at n. This means that g is defined at n.

Finally, we'll show that $g >_* f$ for all $f \in \mathscr{F}$. We know that for any $f \in \mathscr{F}$, we have $G \cap D_f \neq \emptyset$. So there exists $(\phi_f, \mathscr{F}_f) \in G$ such that $f \in \mathscr{F}_f$. Let $\text{dom}(\phi_f) = \{1, 2, \ldots, n\}$. We claim that for any $m > n$, we have $g(m) > f(m)$. If we can prove this claim, we will have shown that $g > *f$.

The value of $g(m)$ will be given by any element $(\phi_m, \mathscr{F}_m) \in D_m$. We know that $(\phi_m, \mathscr{F}_m)$ and $(\phi_f, \mathscr{F}_f)$ are compatible, so they have a common strengthening—let's call it $(\phi_{mf}, \mathscr{F}_{mf})$. Since $(\phi_{mf}, \mathscr{F}_{mf})$ is a strengthening of $(\phi_m, \mathscr{F}_m)$, it is defined at m, and $g(m) = \phi_{mf}(m)$. Since $(\phi_{mf}, \mathscr{F}_{mf})$ is a strengthening of $(\phi_f, \mathscr{F}_f)$, we know that $\phi_{mf}(m) > f(m)$. So we're done! Yaaay! □

2.3 Okay, But How Does This Help?

So we've shown that if there is a filter that intersects with these sets, then we can find a dominating function. But why should we believe that such a filter exists? Well, it seems not entirely implausable that such a thing *could* be true. The sets we have chosen for this intersection are in a technical sense quite large.

[5] Oooohkay. So this is technically correct if you think of a function as a set of ordered pairs. If you don't want to think of a function as a set of ordered pairs, then this means more or less what you'd expect—you glue the functions together. But this is a set theory class. Of *course* you want to think of a function as a set of ordered pairs.

Definition: We say that a subset $D \subseteq \mathbb{P}$ is **dense** iff for any $p \in \mathbb{P}$, there exists $q \in D$ such that $q \leq p$.

So if we pick any element in $\mathbb{P}$, there will always be an element of the dense set below it.

Stupid Example: For any poset $\mathbb{P}$, $\mathbb{P}$ is dense in $\mathbb{P}$.[6]

Less Stupid Example: The set $D_f = \{\phi, \mathscr{F}_0) \mid f \in \text{dom}(\phi)\}$ is dense in $\mathbb{P}_{\mathscr{F}}$.

Another Relevant Example: The set $D_n = \{(\phi, \mathscr{F}_0) \mid n \in \text{dom}(\phi)\}$ is also dense in $\mathbb{P}_{\mathscr{F}}$.

Notice that property (c) says that for any $n \in \mathbb{N}$, $G \cap D_n$ is nonempty. Property (d) says that for any $f \in \mathscr{F}$, $G \cap D_f$ is nonempty. So essentially all that we need to do is find a filter that intersects with a large collection of very large sets. The only question is: how many of these very large sets can we reasonably expect a filter to intersect with?

Fact 1: (ZFC) If $\mathbb{P}$ is a poset and $\{D_n : n \in \mathbb{N}\}$ is a countable collection of dense sets, then there exists a filter $G \subseteq \mathbb{P}$ such that $G \cap D_n \neq \emptyset$ for all $n \in \mathbb{N}$.

Proof. Let $\mathbb{P}$ be a poset, and let $\{D_n : n \in \mathbb{N}\}$ be a countable collection of dense sets. Then there exists a sequence of elements

$$p_0 \geq p_1 \geq \ldots \geq p_n \geq \ldots$$

such that each p_i is an element of D_i. The set $\{q : \exists\ n \in \mathbb{N} \text{ s.t. } q \geq p_n\}$ is a filter. □

On the other hand, if we insisted that G intersect with continuum many dense sets, then we could use the same argument from section 3.1 to show that there exists a function that dominates every function from $\mathbb{N}$ to $\mathbb{N}$, which we know cannot exist. So again, we have a result which behaves very differently in the countable and continuous cases. Let's propose the following axiom:

Proposed Axiom: If $\mathbb{P}$ is a poset, A is a set such that $|A| < |\mathbb{R}|$, and $\{D_\alpha : \alpha \in A\}$ is a collection of dense sets, then there exists a filter $G \subseteq \mathbb{P}$ such that $G \cap D_\alpha \neq \emptyset$.

[6] Yep. Told you it was going to be stupid.

2.4 This Axiom Is Dumb

What's wrong with this axiom? In short: it's not true. If we leave the axiom as written, then our filters are too powerful—they allow us to construct functions which simply cannot exist. We'll go through an example in the homework!

2.5 The Countable Chain Condition

Recall that p and q are **compatible** if there exists a common strengthening of p and q. Otherwise, p and q are **incompatible**, and we write $p \perp q$.

We call a subset A of a poset $\mathbb{P}$ an **antichain** if the elements of A are pairwise incompatible. That is, for any $a, b \in A$, there is no $p \in \mathbb{P}$ satisfying $p \leq a$ and $p \leq b$.

If we think of a poset as a collection of puzzle pieces, then an antichain is a collection of pieces that all belong to different puzzles. There is no way of making a coherent whole out of them. Even if you have less than $2^{\aleph_0}$ dense sets, when the antichains become too large, it becomes impossible to find a filter that intersects with all of them. The common strengthening condition becomes too hard to satisfy with all of these incompatible choices floating around. That was the problem with our poset $\mathbb{P}_{\frown}$. It has enormous (i.e. uncountable) antichains.

We say that $\mathbb{P}$ satisfies the **countable chain condition** if every antichain of $\mathbb{P}$ is countable.[7] We also say "$\mathbb{P}$ is CCC."[8]

Definition: Given a cardinal number κ, we use the notation $\mathrm{MA}(\kappa)$ to stand for the statement: "If $\mathbb{P}$ is a CCC poset and $\{D_\alpha : \alpha \in \kappa\}$ is a collection of dense subsets, then there exists a filter $G \subseteq \mathbb{P}$ such that $G \cap D_\alpha \neq \emptyset$ for all $\alpha \in \kappa$."

Note: We know that $\mathrm{MA}(\aleph_0)$ is true, and that $\mathrm{MA}(2^{\aleph_0})$ is false.

Martin's Axiom: (Real Version) If κ is a cardinal satisfying $\aleph_0 < \kappa < 2^{\aleph_0}$, then $\mathrm{MA}(\kappa)$ is true.

[7] Yes, this is clearly backwards and wrong. It should be the countable *antichain* condition. Don't blame me—I didn't name it.

[8] And yes, this reads "$\mathbb{P}$ is Countable Chain Condition." Really we should never allow logicians to name anything ever. **Optional Homework:** Tell Steve that I said so.

2.6 Our Poset Is CCC!

Proposition: $\mathbb{P}_{\mathscr{F}}$ is CCC.

Proof. There are only countably many finite partial functions ϕ. By the pigeonhole principle, in any uncountable subset of $\mathbb{P}_{\mathscr{F}}$, there exist two elements $(\phi, \mathscr{F}_0)$ and $(\psi, \mathscr{F}_1)$ such that $\phi = \psi$. These two elements have a common strengthening given by $(\phi, \mathscr{F}_0 \cup \mathscr{F}_1)$. Thus no uncountable subset of $\mathbb{P}_{\mathscr{F}}$ is an antichain. It follows that all antichains of $\mathbb{P}_{\mathscr{F}}$ are countable. □

This finishes our discussion of dominating functions. Now that we've shown that $\mathbb{P}_{\mathscr{F}}$ is CCC, our argument from section 3.1 shows that we have the following:

Theorem: (MA) If A is a set such that $|A| < |\mathbb{R}|$, and $\mathscr{F} = \{f_\alpha : \alpha \in A\}$ is a set of functions from $\mathbb{N}$ to $\mathbb{N}$, then there exists a function $g : \mathbb{N} \mapsto \mathbb{N}$ such that $g >_* f_\alpha$ for all $\alpha \in A$.

2.7 Homework!

1. Let x be a nonempty set, and let $\mathbb{P}$ be the collection of nonempty subsets of x, with ordering given by set inclusion.

   (a) For $y, z \subset x$, when do we have $y \perp z$?

   (b) Can you find necessary and sufficient conditions for $\mathbb{P}$ to be CCC?

2. Define a poset $\mathbb{P}_{\frown}$ consisting of partial functions

   $$\phi : \{1, 2, \ldots, n\} \to \{\omega_1\},$$

   ordered by extension. That is, $\phi \geq \psi$ if ψ is an extension of ϕ. For each $n \in \mathbb{N}$, define $D_n = \{\phi : n \in \mathrm{dom}(\phi)\}$, and for each $\alpha < \omega_1$, define $D_\alpha = \{\phi : \alpha \in \mathrm{im}(\phi)\}$.

   (a) Prove that if there exists a filter $G \subseteq \mathbb{P}_{\frown}$ which intersects non-trivially with all D_n and D_α, then this filter defines a surjective function $g : \mathbb{N} \to \omega_1$. (This is a problem.)

   (b) Prove that $\mathbb{P}_{\frown}$ is not CCC.

3 Insane One-Day Intro To Model Theory

3.1 The Language of Set Theory

If we want to be able to prove independence results, we need to be very careful of what we mean when we talk about axioms, theorems, and proofs. When we study set theory, really what we're studying is a collection of statements that can be made in a particular language. This language consists of finite strings of the following symbols:

Relation Symbols: $\in, =$

Connective Symbols: $\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$

Quantifiers: $\forall, \exists$

Parentheses: ()

Variable Symbols: $x, y, z, \alpha, \beta, \gamma, a, b, c,$ etc.

This set of symbols isn't really minimal (see exercises), but it's the collection of symbols we're starting with. We'll occasionally use other symbols, but only as a shorthand for ideas we can build up using these symbols.

3.2 Definition Blitz

Definition: A **language** is a collection of three types of symbols.

- Constant Symbols (We'll usually use a c.)
- Relation Symbols (We'll usually use an r.)
- Function Symbols (We'll usually use an f.)

Each relation symbol and function symbol also comes equipped with an "arity." That is, a relation or function symbol already knows whether it is binary, ternary, unary, zero-ary, or k-ary.

A language always comes automatically equipped with the $=$ relation, the connective symbols, the quantifiers, the parentheses, and countably many variable symbols. So we would write the language of set theory simply as $\mathscr{L}_{\text{ZFC}} = \{\in\}$.

A grammatically-correct sequence of symbols in the language $\mathscr{L}$ is called an $\mathscr{L}$-formula. Examples in $\mathscr{L}_{\text{ZFC}}$ include:

(a) $\forall y \forall x((y \in x) \Rightarrow (\neg(x \in y)))$

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

These examples are a bit different. In example (a), every variable is bound up by one of the $\forall$ quantifiers. This means that once we have an interpretations for these symbols, this formula will either be "true" or "false." We will call this kind of formula a **sentence**, and use the notation ϕ. Example (b) has the variable y bound up by a quantifier, but x and z are running around free. Before we'll be able to determine the truth or falsehood of the formula, we'll need to choose values for x and z. This kind of formula is not a sentence, and we'll use the notation $\phi(x, z)$ to indicate that there are two free variables in the formula. When we need a formula with some number of free variables, but we don't particularly care how many, we'll use the notation $\phi(\overline{x})$.

Definition: Given a language $\mathscr{L}$, and $\mathscr{L}$-structure $\mathscr{M}$ consists of

- A nonempty set M, which we call the underlying set or universe of $\mathscr{M}$.
- Interpretations for each symbol in $\mathscr{L}$.
  - For each constant symbol c, the interpretation is a specific element of M. That is,
  $$c_{\mathscr{M}} \in M.$$
  - For each k-ary relation symbol r, the interpretation is a specific k-ary relation on M. That is,
  $$r_{\mathscr{M}} \in M^k.$$
  - For each k-ary function symbol f, the interpretation is a specific k-variable function. That is,
  $$f_{\mathscr{M}} : M^k \to M.$$

Once we have interpretations of all the language symbols in $\mathscr{M}$, we have the ability to determine whether a sentence ϕ is true or false in $\mathscr{M}$.

Definition: If ϕ is true in $\mathscr{M}$, then we write $\mathscr{M} \models \phi$, and say that $\mathscr{M}$ **models** or **satisfies** ϕ.

Definition: A **theory** $\mathscr{T}$ is a collection of sentences in the language $\mathscr{L}$. Given a theory $\mathscr{T}$ and an $\mathscr{L}$-structure $\mathscr{M}$, we write $\mathscr{M} \models \mathscr{T}$ if for every $\phi \in \mathscr{T}$, we have $\mathscr{M} \models \phi$. In this case, we say that $\mathscr{M}$ is a **model** of the theory $\mathscr{T}$.

Definition: Given a sentence ϕ, we say that $\mathscr{T}$ proves ϕ, and write $\mathscr{T} \vdash \phi$. If there exists ϕ such that $\mathscr{T} \vdash \phi$ and $\mathscr{T} \vdash (\neg\phi)$, then we say that $\mathscr{T}$ is **inconsistent**. Otherwise, we say that $\mathscr{T}$ is **consistent**.

3.3 Interlude: Completeness and Universe Existence

By some strange miracle of mathematics[9], a theory $\mathscr{T}$ in a well-orderable[10] language $\mathscr{L}$ is consistent if and only if there exists an $\mathscr{L}$-structure $\mathscr{M}$ such that $\mathscr{M} \models \mathscr{T}$.

One direction of this implication is obvious. If a theory is inconsistent, it makes sense that there should be no models of that theory. The miraculous part is that whenever a theory is consistent, it is possible to build a model. In particular, if ZFC is consistent[11], then there exists some $\mathscr{L}_{\text{ZFC}}$-structure $\mathscr{U}$ such that $\mathscr{U}$ models ZFC. However $\mathscr{U}$ is not the universe. It's a set. It's way to small to contain the entire set-theoretic universe.

3.4 Relationships Between $\mathscr{L}$-Structures

Definition: Let $\mathscr{M}$ and $\mathscr{N}$ be $\mathscr{L}$-structures. We say that $\mathscr{M}$ is a **substructure** of $\mathscr{N}$, and that $\mathscr{N}$ is an **extension** of $\mathscr{M}$ if the following conditions hold:

- M, the underlying set of $\mathscr{M}$, is a subset of N, the underlying set of $\mathscr{N}$.
- For a k-ary function symbol f and $m_1, \ldots, m_k \in M$, we have

$$f_{\mathscr{N}}(m_1, \ldots, m_k) = f_{\mathscr{M}}(m_1, \ldots, m_k).$$

[9] Technically, the result we're citing here is Gödel's completeness theorem. Not to be confused with Gödel's incompleteness theorem. We won't prove this theorem in this class, but a good development is available at https://terrytao.wordpress.com/2009/04/10/the-completeness-and-compactness-theorems-of-first-order-logic/

[10] This condition is irrelevant because we're assuming choice.

[11] And it'd better be, or we're in trouble.

- For a k-ary relation symbol r and $m_1, \ldots, m_k \in M$, we have

$$r_{\mathscr{N}}(m_1, \ldots, m_k) \Leftrightarrow r_{\mathscr{M}}(m_1, \ldots, m_k).$$

We call $\mathscr{M}$ an **elementary substructure** of $\mathscr{N}$, and we call $\mathscr{N}$ an **elementary extension** of $\mathscr{M}$ if in addition,

- Given $m_1, \ldots, m_k$, and some formula $\phi(x_1, \ldots, x_k)$, we have

$$\mathscr{N} \models \phi(m_1, \ldots, m_k) \;\Leftrightarrow\; \mathscr{M} \models \phi(m_1, \ldots, m_k)$$

This means that whenever a proposition regarding some collection of elements in M is true in $\mathscr{M}$, that same proposition remains true about the same collection of elements when we pass to the larger structure $\mathscr{N}$. In particular, the same collection of sentences is true in $\mathscr{M}$ and $\mathscr{N}$.

Proposition: (Tarski-Vaught) Let $\mathscr{M}$ be a substructure of $\mathscr{N}$. We have $\mathscr{M} \preceq \mathscr{N}$ if and only if for any formula $\phi(x, \overline{y})$ and $\overline{m} \in M$, whenever there exists $n \in N$ such that $\mathscr{N} \models \phi(n, \overline{m})$, there also exists $n' \in M$ such that $\mathscr{N} \models (n', \overline{m})$.

The Tarski-Vaught criterion is often described as "$\exists$'s go down." The idea is that a sentence with no quantifiers will obviously be true in $\mathscr{M}$ if and only if it is true in $\mathscr{N}$. Any existential statement that is true in $\mathscr{M}$ will be true in $\mathscr{N}$, since whenever there exists an $m \in M$ such that something is true, that same m is also an element in N, and the statement will be true for the same reason. So the only problem that we could possibly encounter would be an existential statement that is true in $\mathscr{N}$ but not in $\mathscr{M}$.[12]

3.5 The Löwenheim-Skolem Theorem

Theorem: If a theory $\mathscr{T}$ in a countable language $\mathscr{L}$ has an infinite model $\mathscr{N}$, then there exists a countable model $\mathscr{M}$ such that $\mathscr{M} \preceq \mathscr{N}$.

Idea: A substructure is going to have to be closed under all the functions in $\mathscr{L}$. This is easy to do. We start with the interpretations of the constant symbols, plug them into the functions in $\mathscr{L}$ and add them to M. Then we

[12] This is a good argument for why the Tarski-Vaught test works, but not quite a proof. The proof will involve inducting on the length of $\mathscr{L}$-formulas.

do it again. We'll need to run down the details to make sure that this process will someday end, but this is easy.[13]

In order for the substructure to be elementary, it needs to satisfy all the same existential statements as the bigger model. This is not easy to do.[14] But we can turn it into the easy problem. The key to this proof is expanding our language $\mathscr{L}$ to include an extra function f_ϕ for eah $\phi(x, \overline{y})$, which will be interpreted such that whenever $\exists x \phi(x, \overline{m})$ is true in $\mathscr{N}$, $f_\phi(\overline{m})$ will run out and find us an element $n \in N$ that makes $\phi(n, \overline{m})$ true.[15] Once we have our expanded language and our expanded theory, closing M under our new and improved collection of functions will give us an elementary submodel. And if we're lucky, it won't be too big.

Proof. We'll begin by defining our expanded language $\mathscr{L}_*$. We'll do so by building a countable sequence of languages

$$\mathscr{L} = \mathscr{L}_0 \subseteq \mathscr{L}_1 \subseteq \mathscr{L}_2 \subseteq \dots$$

recursively as follows: Given $\mathscr{L}_i$, we allow

$$\mathscr{L}_{i+1} = \mathscr{L}_i \cup \{f_\phi : \phi(x, \overline{y}) \text{ an } \mathscr{L}_i\text{-formula}\}$$

with each f_ϕ a function symbol of the correct arity k. In the model $\mathscr{N}$, f_ϕ will be interpreted to be a function from N^k to N such that if there exists $n \in N$ such that $\mathscr{N} \models \phi(n, \overline{m})$, then $\mathscr{N} \models \phi(f_\phi(\overline{m}), \overline{m})$. (If multiple appropriate elements of N exist, pick one.) If there is no such n, then arbitrarily assign $f_\phi(\overline{m})$ a value in N. This gives $\mathscr{N}$ an interpretation as an $\mathscr{L}_*$ structure.

Each formula ϕ has finite length, and we have at most countably many choices for each symbol in ϕ. This means that in each step, we add at most countably many function symbols to our language. Thus all of the $\mathscr{L}_i$ are countable languages, and if we define $\mathscr{L}_* = \bigcup_{i \in \omega} \mathscr{L}_i$, then $\mathscr{L}_*$ is a countable language.

Now that we've defined $\mathscr{N}$ as a structure in our new language $\mathscr{L}_*$, we are ready to define our substructure $\mathscr{M}$. We start by defining a sequence

$$\emptyset = X_0 \subseteq X_1 \subseteq X_2 \subseteq \dots$$

of subsets of N by setting

$$X_{i+1} = X_i \cup \{f_{\mathscr{N}}(\overline{x}) : f \text{ an } \mathscr{L}_*\text{-function}, \overline{x} \in X_i\}$$

[13] For sufficiently large values of "easy."

[14] For sufficiently small values of "easy."

[15] The f is for fetch!

Since there are only countably many symbols in $\mathscr{L}_*$, we are adding at most countably many elements in each step.

We will define $\mathscr{M}$ to be the $\mathscr{L}_*$ substructure of $\mathscr{N}$ with underlying set

$$M = \bigcup_{i \in \omega} X_i.$$

This is clearly a countable set, so we only need to verify that $\mathscr{M}$ is an elementary substructure of $\mathscr{N}$.

To show that M is an $\mathscr{L}_*$-substructure, we need to show that for any function $f \in \mathscr{L}_*$, and for any $\overline{m} \in M$, we have $f_{\mathscr{N}}(\overline{m}) \in M$. Since $\overline{m} \in M$, there exists i such that $\overline{m} \in X_i$. It follows that $f(\overline{m}) \in X_{i+1}$, and thus $f(\overline{m}) \in M$.

To show that this substructure is elementary, we must show that for any $\phi(x, \overline{y})$, and for any $\overline{m} \in M$, whenever there exists $n \in N$ with $\mathscr{N} \models \phi(n, \overline{m})$, there also exists $n' \in M$ with $\mathscr{N} \models \phi(n', \overline{m})$. We have $(f_\phi)_{\mathscr{N}}(\overline{m}) \in M$ because $\mathscr{M}$ is an $\mathscr{L}_*$-substructure of $\mathscr{N}$. And by construction, $\mathscr{N} \models \phi((f_\phi)_{\mathscr{N}}(\overline{m}), \overline{m})$. Thus our proof is complete. $\square$

3.6 Homework!

1. Write out what it means for a set x to be the powerset of a set y in the formal language of set theory. Why do you suppose it is possible for a model of ZFC to satisfy the Powerset axiom, and yet be countable?

2. Show that if $\mathscr{M}_0$, $\mathscr{M}_1$, and $\mathscr{M}_2$ are $\mathscr{L}$-structures such that $\mathscr{M}_0 \preceq \mathscr{M}_1$ and $\mathscr{M}_1 \preceq \mathscr{M}_2$, then $\mathscr{M}_0 \preceq \mathscr{M}_2$.

3. Show that the quantifier symbol $\forall$ is unnecessary—it can be rewritten in terms of logical connectives and the $\exists$ symbol.

4. A formula ϕ is called **atomic** if it takes the form $r(\overline{x})$ for some collection of variables $\overline{x}$.

   Let $\mathscr{M}$ be a substructure of $\mathscr{N}$. Prove that any atomic formula is true in $\mathscr{M}$ if and only if it is true in $\mathscr{N}$.

5. A formula ϕ is **quantifier-free** if it has no quantifiers.

   Let $\mathscr{M}$ be a substructure of $\mathscr{N}$. Prove that any quantifier-free formula is true in $\mathscr{M}$ if and only if it is true in $\mathscr{N}$. (Hint: Induct on the length of the formula.)

6. Prove the Tarski-Vaught theorem. That is, show that if $\mathscr{M}$ and $\mathscr{N}$ satisfy the Tarksi-Vaught criterion, then for any formula $\phi(\overline{x})$ and $\overline{m} \in \mathscr{M}$, we have that $\phi(\overline{m})$ is true in $\mathscr{M}$ if and only if it is true in $\mathscr{N}$. (Hint: induct on the number of quantifiers.)

4 Mostowsky Collapse

4.1 Transitivity

Assume we have a countable model $\mathscr{A}$ of set theory, in which $\in_{\mathscr{A}}$ is the actual relation $\in$. (We showed yesterday that we can get this from Löwenheim-Skolem. That model comes with a bunch of other odd properties, but we'll mostly be interested in the countable-ness and the niceness of $\in_{\mathscr{A}}$.)

Our model $\mathscr{A}$ still has the potential to be pretty frustrating. For example, suppose $a \in A$, and $A \models \neg\exists x(x \in a)$. Then $\mathscr{A}$ believes that a is the emptyset. But a doesn't have to be the emptyset. It could be the set $a = \{b, c, d\}$, with $b, c, d \notin A$. This is inconvenient, to say the least.[16] We want to be able to avoid having sets in our model with secret invisible elements that our model doesn't know about.

Definition: A model $\mathscr{M}$ is **transitive** if whenever $m \in M$, and $n \in m$ we have $n \in M$.

This solves our empty set problem. If $a = \{b, c, d\}$ and $a \in A$, then $b, c, d \in A$, and there's no way $\mathscr{A}$ is going to accidentally think that a is empty.

But how do we get a transitive universe?

4.2 The Von Neumann Heirarchy

Let's pretend for a moment to be working in the actual set-theoretic universe. [17] We define the following collection of sets:

$$\begin{array}{lcll} V_0 & = & \emptyset & \\ V_{\alpha+1} & = & \mathscr{P}(V_\alpha) & \text{for every ordinal number } \alpha \\ V_\beta & = & \bigcup\limits_{\alpha<\beta} V_\alpha & \text{for every limit ordinal } \beta \end{array}$$

The axiom of foundtation tells us that every set in our universe is contained in one of these V_α's. Using this fact, we can define something called the "rank" of a set:

[16] I would say terrible, or tragic, but I rarely say the least.

[17] Or an existing model of ZFC that we're currently pretending is the universe. Whatevs. Yay model theory.

$$\text{rank}(x) = \min\{\alpha \mid x \in V_{\alpha+1}\}.$$

The rank gives us a way of determining which sets are "allowed" to be elements of which other sets. Specifically, we have:

Theorem: If $y \in x$, then rank(y) <rank(x).

Proof. We will induct[18] on the rank of x.

If rank$(x) = 0$, then $x = \emptyset$, so the result holds. Now assume that

$$\text{rank}(x) = \alpha > 0,$$

and the result holds for all smaller ranks. Since rank$(x) = \alpha$, we know that

$$x \in V_{\alpha+1} = \mathscr{P}(V_\alpha).$$

Thus if $y \in X$, then $y \in V_\alpha$, and so

$$\text{rank}(y) < \alpha = \text{rank}(x).$$

□

4.3 The Mostowsky Collapse Function

Now let's take our model $\mathscr{A}$, and define a "function" G on the set A by setting

$$G(x) = \{G(y) : y \in A \cap x\}$$

We'll define $M = \text{Im}(G)$, and $\mathscr{M}$ to be the $\mathscr{L}_{\text{ZFC}}$-structure given by interpreting $\in_{\mathscr{M}}$ to be the actual $\in$ relation. We intend to prove the following:

(i) There is totally nothing sketchy going on in the definition of G.

(ii) M is a countable transitive model of ZFC.

Proof of (i). We define G recursively, inducting on the 'rank" of x. But not the real rank of x! The ordinal that $\mathscr{A}$ *believes* is the rank of x. If

$$\mathscr{A} \models \text{rank}(x) = 0,$$

[18]This is a relatively simple transfinite induction argument

then we have

$$\mathscr{A} \models x = \emptyset,$$

so we know that $x \cap A = \emptyset$. Thus,

$$G(x) = \{G(y) \mid y \in \emptyset\} = \emptyset.$$

So we can define $G(x)$ for all x that $\mathscr{A}$ believes to be rank-zero. Now assume

$$\mathscr{A} \models \text{rank}(x) > 0,$$

and that we have defined $G(y)$ for all y with

$$\mathscr{A} \models \text{rank}(y) < \text{rank}(x).$$

Then $G(y)$ is defined for all y such that

$$\mathscr{A} \models y \in x,$$

and thus for all $y \in A \cap x$. Thus our definition of $G(x)$ makes sense. □

Proof of (ii). Since M is the image under G of a countable set, M is countable. Since all elements of $G(x)$ take the form $G(z)$ for some $z \in A$, M is transitive. But is M a model of ZFC? Well sure it is! For any $x, y \in A$ we have

$$(G(x) \in G(y)) \Leftrightarrow x \in y,$$

so essentially M behaves the same way that A behaves—we've just shifted the labels around some. □

So now we've proved that there exists a countable transitive model of set theory!

4.4 Building Our Instinct For Absoluteness

One of the things that we definitely won't have time to do in this class is verify that each statement we're working with is absolute in our countable transitive model of ZFC. However, we can develop an instinct for what sorts of statements "should" be absolute.

Our best friend here is the transitivity of our model. Transitivity means that the sentence $x \in y$ is always absolute. Our biggest problems are the $\forall$ and $\exists$ symbols, since our funny model has a bunch of pieces missing. Here are some examples to get us thinking in the right direction:

(a) If $x \in M$ and $y \in M$ and $\mathscr{U} \models x \subseteq y$, then $\mathscr{M} \models x \subseteq y$.[19]

(b) If $x \in M$ and y is a finite subset of x, then $y \in M$, and $M \models x \subseteq y$.

(c) Any element that can be constructed from sets in M using the ZFC axioms is an element of M, since $\mathscr{M} \models$ZFC. However, the set that is constructed may not be the same set in $\mathscr{M}$ as it is in $\mathscr{U}$. For example, given a set x in M, there exists a set y in M such that

$$\mathscr{M} \models x \text{ is the powerset of } y$$

but this may not be the powerset of x as defined in $\mathscr{U}$.

(d) Any element that can be constructed entirely within $\mathscr{M}$ will exist in $\mathscr{M}$. However, if there is a set that can only be proven to exist by stepping outside $\mathscr{M}$ to look at the "real world," that set may not be an element of $\mathscr{M}$.[20]

4.5 And Now Back To Posets!

Here it will be useful to think of posets as ordered triples $(\mathbb{P}, \leq, \mathbb{1})$, where the additional symbol $\mathbb{1}$ is the largest element of $\mathbb{P}$. As usual, we will consider $\mathbb{P}$ to be a poset of partial information about a particular object of interest.

Suppose $(\mathbb{P}, \leq, \mathbb{1}) \in M$. We call the filter $G \subseteq \mathbb{P}$ a **$\mathbb{P}$-generic** filter over M if whenever $D \subseteq \mathbb{P}$ is dense in $\mathbb{P}$ and $D \in M$, we have $D \cap G \neq \emptyset$. This looks sort of like the filters we used in our Martin's Axiom arguments, but instead of intersecting with a certain (countable) number of carefully chosen dense sets, this thing just intersects with *all* the dense sets! All of them! This filter does everything any filter could possibly do. Now—why on earth should such a thing exist?

Well, it kinda shouldn't. But in the real world, M has only a countable number of elements. Which means that there are only countably many dense sets $D \in M$. And in the real world, MA(ω) is true. This means that in the real world, $\mathbb{P}$-generic filters exist. Next time, we'll prove that our $\mathbb{P}$-generic filter can only exist inside M if our poset $\mathbb{P}$ is *extremely* boring.

[19]Proof: Exercise! Hint: Transitivity!

[20]This will be the last time that we use the symbol $\mathscr{M}$. This is because in future sections, it will become more and more inconvenient to distinguish between the model $\mathscr{M}$ and the underlying set M. So. I hope you've enjoyed our pretty $\mathscr{M}$, but it's time to say goodbye and move on.

4.6 Homework!

For some of these problems, the ZFC axioms will be super helpful. I've included a copy of them for you on a separate sheet. Feel free to find me at TAU if you're having trouble parsing any of them!

1. Prove that according to ZFC, each set in the universe falls into one of the V_α sets in the Von Neumann heirarchy. Here are some thoughts on how this might be accomplished:

   (a) Let x be a set. First let's build a countable sequence of sets

   $$x = x_0 \subseteq x_1 \subseteq x^2 \subseteq \dots$$

   by setting

   $$x_i = x \cup \{z : \exists y(y \in x) \wedge (z \in y)\}$$

   We take $x_* = \cup_{i \in \omega} x_i$. Prove that x_* is transitive.

   (b) Prove that each set in x_* are in some V_α, then so is x.

   (c) Otherwise, define $u \subset x_*$ to be the collection of unranked sets. The axiom of foundation indicates that u must contain an element w such that $w \cap u = \emptyset$. Use this to derive a contradiction.

2. Prove that the statement $x \subseteq y$ is absolute in $\mathscr{M}$.

3. Prove that the statement $x = \bigcup_{y \in z} y$ is absolute in $\mathscr{M}$.

4. Prove that the statement "x is an ordinal number." is absolute in $\mathscr{M}$. (Recall that an ordinal number is defined to be a transitive set which is well-ordered under the $\in$ relation.)

5. Prove that if $x \in M$, and y is a finite subset of x, then $y \subseteq M$.

6. Prove that the statement "x is ω" is absolute in $\mathscr{M}$.

7. Explain why the statement "x is ω_1" cannot be absolute in $\mathscr{M}$.

5 Model Extensions

5.1 Posets Don't Have Generic Filters

At least, not if the posets are even remotely interesting. Let's go ahead and say that we'll consider $\mathbb{P}$ "interesting" if $\mathscr{M}$ satisfies the statement, "for all $p \in \mathbb{P}$, there exist q and r with $q \leq p$, $r \leq p$, and $q \perp r$. That is, any element of the poset has incompatible elements below it.

So if we're thinking of our poset as a collection of puzzle pieces, any piece that we choose must be a piece of two very different final pictures. No matter how far down in the poset you go, there are still choices left to be made. By contrast, in an uninteresting poset, you get to a certain point and say, "Oh yeah, that's a bunch of ferrets playing poker. We can stop building now—I know what it's going to look like." If we want to build interesting set-theoretic objects, we will need to use interesting posets.

Fact: If $\mathbb{P}$ is interesting and $G \subseteq \mathbb{P}$ is $\mathbb{P}$-generic, then $G \notin M$.

Proof. Suppose $G \in M$. Since $\mathbb{P} \in M$ and $\mathscr{M} \models \text{ZFC}$, it follows that $\mathbb{P} \setminus G$ is an element of M. For ease of notation,[21] set $D = \mathbb{P} \setminus G$. Let p be an arbitrary element of $\mathbb{P}$. By assumption, there exist strengthenings q and r of p such that $q \perp r$. At least one of these—say q is not in G. Thus $q \in D$. We've just shown that for any $p \in \mathbb{P}$, we can find a $q \leq p$ such that $q \in D$. It follows that D is a dense set with $D \cap G = \emptyset$. Contradiction![22] □

So we have this generic filter G out in the real world, but we can't really build anything with it yet, because it's not in our model. Our mission, should we choose to accept it, is to create a countable transitive model (CTM) that contains both M and G.[23] This will take a considerable amount of time and effort, but it will bring us right to the doorstep of the proof of the independence of the continuum hypothesis.

[21] And a hint as to how this proof is about to work.

[22] Oh noes!

[23] Two different kinds of contains are happening here. Because English is terrible.

5.2 Masters of the Universe

Since $\mathscr{M}$ is a transitive model, every element of every set in M is also an element of M. Since $\mathbb{P} \in M$ and $G \subseteq \mathbb{P}$, it follows that $G \subseteq M$. And yet somehow $G \notin \mathbb{P}$. So what goes wrong?

The answer is: even though elements never go missing, subsets do. There is nothing in ZFC that can explicitly say that all subsets of a given set exist. An infinite set has an uncountable number of subsets, and a first-order language only has sentences to describe countably many of them.

What we have here is a teeny-weeny universe M sitting inside the real world. We, being masters of the unverse, can see all of the subsets that exist everywhere, but the people living inside M can't see the missing sets.

But perhaps—just perhaps they've heard whispers of a wider universe, $\mathscr{M}[G]$, which for them only exists in legends. But the people of $\mathscr{M}$ have names for the legendary sets of $\mathscr{M}[G]$—names that would have a meaning if only someone could tell them what G was.

5.3 $\mathbb{P}$-Names

We call τ a $\mathbb{P}$-name if

(i) τ is a set of ordered pairs (σ, p).

(ii) For any $(\sigma, p) \in \tau$, σ is a $\mathbb{P}$-name, and $p \in \mathbb{P}$.

Note: Here's an alternate definition. I haven't decided what I like better. We can define $\mathbb{P}$-names recursively as follows:

(i) $\emptyset$ is a $\mathbb{P}$-name.

(ii) Any collection of elements of the form (τ, p) with τ a $\mathbb{P}$-name and $p \in \mathbb{P}$ is a $\mathbb{P}$-name.

So obviously, $\emptyset$ is a $\mathbb{P}$-name. And this means that for any $p \in \mathbb{P}$ is a $\mathbb{P}$-name. We can build all the larger $\mathbb{P}$-names from the smaller $\mathbb{P}$-names. Note that "being a $\mathbb{P}$-name" is a an absolute property, since it only relies on the $\in$ relation. We use the notation $M^{\mathbb{P}}$ for the set of all $\mathbb{P}$-names in M.

Now let $G \subseteq \mathbb{P}$ be a $\mathbb{P}$-generic filter, and let $\tau \in M^{\mathbb{P}}$. As the name would suggest, a $\mathbb{P}$ name ought to be a name for something. However, without access

to G, we can't figure out what. We define the **interpretation** of a $\mathbb{P}$-name τ to be

$$\tau_G = \{\sigma_G \mid \exists\ p \in G \text{ such that } (\sigma, p) \in \tau\}.$$

So if we told the people of M where to find G, they could actually build all the interpretations of τ_G by starting with τ, throwing away the pairs whose second coordinate is not in G, and using the first coordinate of the remaining $\mathbb{P}$-names.

$\mathbb{P}$-names do a great job of building on each other recursively. Since $\emptyset$ is a $\mathbb{P}$-name, we have $\mathbb{P}$-names whose first coordinates are the $\mathbb{P}$-names corresponding to elements of $V_\emptyset$. From those, we can build $\mathbb{P}$-names whose first coordinates represent things in V_1. From there we can get V_2, and keep going to get V_α for all ordinal numbers α. This means that we've got names floating around for all the sets in M, plus some extra subsets from G which can pop out of the interpretations. Exciting!

Definition: $M[G] = \{\tau_G : \tau \in M^{\mathbb{P}}\}$, and $\mathscr{M}[G]$ is this set equipped with the $\in$ relation from the ambient universe.

As it turns out, $\mathscr{M}[G]$ is the smallest possible countable transitive model containing both M and G. This takes a *lot* of checking. Fortunately, for our purposes it's good enough to verify that $\mathscr{M}[G]$ is a countable transitive model of ZFC containing M and G.

Note: If this $\mathbb{P}$-name thing seems super weird, that's because it is. Don't worry—as we go, we'll get a better sense for what these $\mathbb{P}$-names are and what they can do.

5.4 $M \subseteq M[G]$

For each $x \in M$, we define

$$\check{x} = \{(\check{y}, \mathbb{1}) \mid y \in x\}.$$

Since G is closed upward, we know that $\mathbb{1} \in G$, and so $\check{x}_G = x$. This menas that $M \subseteq M[G]$.

5.5 $G \in M[G]$

To show that $G \in M[G]$, we set

$$\Gamma = \{(\check{p}, p) \mid p \in \mathbb{P}\}.$$

Thus Γ_G, the interpretation of Γ, will contain exactly the elements $\check{p}$ for $p \in G$.

5.6 $M[G]$ is a CTM

Aaand this is the unpleasant part. We need to show that $M[G]$ is countable and transitive, which doesn't take too long. But then we need to show that $M[G]$ satisfies all of the axioms of ZFC. This will take a while, but let's start by doing the easy bits.

5.7 The Easy Bits

Countability:

$M[G]$ contains at most one interpretation for each $\mathbb{P}$-name. All the $\mathbb{P}$-names exist in M, which is countable. So $M[G]$ must be countable as well.

Transitivity:

Suppose $x \in M[G]$, and $z \in x$. We know that $x = \tau_G$, where $\tau \in M^{\mathbb{P}}$. We have

$$\tau_G = \{\sigma_G \mid \exists\ (\sigma, p) \in \tau,\ p \in G\}.$$

Thus $z = \sigma_G$ for some $\sigma \in M^{\mathbb{P}}$, and by definition $z \in M[G]$.

Extensionality:

The axiom of extensionality states that two sets are equal if and only if they contain the same elements. Since $M[G]$ exists inside the standard set-theoretic universe, it will determine set equality in the same way.

Pairing:

The axiom of pairing states that if x and y are sets, then there exists a set of the form $\{x, y\}$. To see that this holds in $M[G]$, take twoo arbitrary $x, y \in M[G]$. We want to show that $\{x, y\} \in M[G]$. We know that $x = \tau_G$ and $y = \sigma_G$ for some $\tau, \sigma \in M^{\mathbb{P}}$. We take the $\mathbb{P}$-name

$$\xi = \{(\tau, \mathbb{1}), (\sigma, \mathbb{1})\}.$$

Since G is closed upwards, $\mathbb{1} \in G$, and so

$$\xi_G = \{\tau_G, \sigma_G\} = \{x, y\}.$$

Foundation:

Foundation isn't super important for the proper functioning of mathematics, but still worth checking. Foundation states that every nonempty set must contain at least one element which is disjoint from itself.

Each set x in $M[G]$ is a real set in the ambient universe, and so must contain an element y that is disjoint from x. Since $M[G]$ is transitive, y is also an element of $M[G]$. Since $y \in x$, and $y \cap x = \emptyset$ are absolute properties, foundation holds in $M[G]$.

Infinity:

The axiom of infinity states that there exists a set x such that $\emptyset \in x$, and such that for any $y \in x$, the set $y \cup \{y\}$ is also in x. Such a set exists in M—we call it ω. And $\check{\omega}_G$ is still ω, since it is the set of $\check{n}$ for every finite ordinal n, all of which we know to exist in our original model $\mathscr{M}$.

Union:

The axiom of union states that given any set z there exists a set y which consists of the elements of elements of z. That is,

$$y = \bigcup_{x \in z} x.$$

Let $z \in M[G]$. Then $z = \tau_G$ for some $\mathbb{P}$-name τ. Let

$$\pi = \bigcup \{\sigma \mid \exists p \in \mathbb{P}, (\sigma, p) \in \tau\}.$$

Clearly, $\pi \in M^{\mathbb{P}}$. Now consider $\pi_G \in M[G]$. For any $x \in z$, we have $x = \sigma_G$ for some σ with $(\sigma, p) \in \tau$ and $p \in G$. It follows that $x \subseteq \pi_G$. It follows that any element $x \in z$ is a subset of π_G. This gives us $\bigcup z \subseteq \pi_G$, and thus there exists $y \in M[G]$ such that $\bigcup z \subseteq y$. If we can show that $y \subseteq z$ as well, we'll be done!

Unfortunately we don't quite seem to have the machinery we need to do that yet. The separation axiom would give it to us, but we need more tools in our toolkit before we can attack separation.

6 Forcing—Yaaay Forcing!

6.1 The Idea Of Forcing

The $\mathbb{P}$-names have gotten us some mileage, but we're still a long way from being able to prove that $M[G]$ is a CTM. And that's not surprising—there's a huge amount of power here that we haven't even begun to harness.

Remember the big-picture story: we're using aoppl[24] filter G in the poset $\mathbb{P}$ in order to build something. But what we're building in this case is a whole set-theoretic universe! And just as in $\mathbb{P}_{\mathscr{F}}$, the elements of the filter gave us partial information about the function we were building, the elements in G ought to be able to give us information about the universe that we're building.

For instance, maybe the element $p \in \mathbb{P}$ is a puzzle piece that tells me, "This universe contains unicorns!" Then if p is in G, we know that we're building a universe with unicorns in it.

Formally, if $\phi(x_1, \ldots, x_n)$ is a first-order formula in the language of set theory with free variables $x_1, \ldots, x_n$ and $\tau_1, \ldots, \tau_n$ are $\mathbb{P}$-names, we write

$$p \Vdash \phi(\tau_1, \ldots, \tau_n)$$

and say p **forces** $\phi(\tau_1, \ldots \tau_n)$ if for every $\mathbb{P}$-generic filter $G \subseteq \mathbb{P}$, we have

$$(p \in G) \Rightarrow (M[G] \models \phi(\tau_{1_G}, \ldots, \tau_{n_G})).$$

We are going to need to be able to prove two things:

- If G is a $\mathbb{P}$-generic filter over $\mathscr{M}$, then we have

$$\mathscr{M}[G] \models \phi(\tau_{1_G}, \ldots, \tau_{n_G}) \Leftrightarrow (\exists p \in G)(p \Vdash \phi(\tau_1, \ldots, \tau_n))$$

- The forcing relation is a relation that we can define *inside* the model $\mathscr{M}$.

However, before we do all that work, let's at least show that in principle, forcing is useful.

[24] The cat walked across my keyboard here. Thought I'd leave it for your amusement.

6.2 Why Forcing is Useful: Separation

So we tried to prove the axiom of union, and we got stuck because we needed separation to get us the rest of the way. Separation states that, given a set a a formula $\phi(x, \overline{y})$, and some other values $\overline{b}$, there exists a set b consisting of all of the elements of a for which $\phi(a, \overline{b})$ is true.

For example, if we have a set y such that $\bigcup z \subseteq y$, we can form a set out of all of the elements x satisfying

$$\exists w((w \in z) \wedge (x \in w)),$$

and obtain the set $\bigcup z$.

To prove that separation holds in $M[G]$, we want to show that whenever $\sigma, \tau_1, \ldots, \tau_n$ are $\mathbb{P}$-names and $\phi(x, y_1, \ldots, y_n)$ is a formula, the set

$$\{a \in \sigma_G : M[G] \models \phi(a, \tau_{1_G}, \ldots, \tau_{n_G})\}$$

is in $M[G]$. We start by defining the set ξ to consist of all ordered pairs (π, p) such that

(i) (π, p) appears as one of the ordered pairs in σ.

(ii) $p \Vdash (\pi \in \sigma) \wedge \phi(\pi, \tau_1, \ldots \tau_n)$.

Now we need to be careful, becuase this set only exists if we can define the $\Vdash$ relation without reference to the larger model. But let's assume for the moment that we can, and that the set ξ is in M, and is a $\mathbb{P}$-name.

ξ_G will consist of the π_G for which $(\pi, p) \in \xi$ for some $p \in G$. The π's in question were candidates for elements of the set σ_G. The ones that will actually make it into ξ_G are all coupled with p's that force both $\pi \in \sigma$ and $\phi(\pi, \tau_1, \ldots, \tau_n)$.

Thus the elements of ξ_G will be elements of $\pi_G \in \sigma_G$ that satisfy $\phi(\pi_G, \tau_{1_G}, \ldots, \tau_{n_G})$. In addition, we must have all such elements, because the if-and-only-if condition of our forcing theorem says that any such element in $M[G]$ has an element of G that forces it to satisfy those two conditions.

It follows that ξ_G is exactly the subset we're looking for.

6.3 Why Forcing Is Hard

Our current definition of the forcing relation is

$$(p \Vdash \phi) \Leftrightarrow (\text{For any } \mathbb{P}\text{-generic } G \text{ with } p \in G,\ M[G] \models \phi.)$$

This is *very* not defined in M. I mean, it *super* references stuff that doesn't exist in M.

The surprising fact about the forcing relation $\Vdash$ is that in spite of the fact that it makes reference to things that happen with various $\mathbb{P}$-generic filters that are definitely *not* contained in M, the relation itself is definable in the small model M. That is to say, even though the people in M don't know what G is, they can make statements of the form, "If p is an element of G, then the universe $M[G]$ would have a set that looks like this!" It turns out that being able to make this kind of statement is exactly what we need in order to finish proving that $M[G]$ is a model of ZFC.

6.4 Dense Below p

In order to define $\Vdash$ inside our model M, we'll need to be able to talk about what it means for a subset of a poset $\mathbb{P}$ to be **dense below** a particular element $p \in \mathbb{P}$. Recall that a subset $D \subseteq \mathbb{P}$ is **dense** if we can "get to" D from anywhere in the poset. That is, for any $x \in \mathbb{P}$, there exists $y \leq x$ with $y \in D$.

But sometimes it doesn't matter so much whether we can get into D from anywhere in the poset—sometimes we'll be satisfied if we can get there from anywhere in the poset that's below a specific element p.

Definition: We say that a set $E \subseteq \mathbb{P}$ is **dense below** p if for any $x \leq p$, there exists $y \leq x$ with $y \in E$.

Notice: A subset D is dense in $\mathbb{P}$ if it is dense below $\mathbb{1}$.

Lemma: Let M be a CTM with $\mathbb{P} \in M$, and $E \subseteq \mathbb{P}$ such that $E \in M$. Let G be $\mathbb{P}$-generic over M. Then the following hold:

(i) Either $E \cap G \neq \emptyset$ or there exists $q \in G$ such that $q \perp r$ for any $r \in E$.

(ii) If $p \in G$, and E is dense below p, then $G \cap E \neq \emptyset$.

Before we prove this lemma, let's talk briefly about what it means. Essentially, a single element of our filter can be extremely powerful. A single element $q \in G$ which is incompatible with the elements of E will force G to never intersect with E at all. On the other hand, if E is dense below a particular element $p \in G$, then G will certainly intersect with E somewhere. This allows us to

look at a single element of G for information about how the entire filter will behave. In particular, you could imagine that a single element p being in G might *force* a particular thing to happen in the final model $M[G]$.

Proof of Lemma: Define the set D to be the union of

$$\{q \in \mathbb{P} \mid \text{ there exists } r \in E \text{ such that } q \leq r\}$$

and

$$\{q \in \mathbb{P} \mid q \perp r \text{ for all } r \in E\}$$

Let $q \in \mathbb{P}$ be arbitrary. If $q \notin D$, then there exists $r \in E$ such that q and r are compatible, since q is not in the second set. Let $p \in \mathbb{P}$ such that $p \leq q$ and $p \leq r$. Since $p \leq r \in E$, we have $r \in D$. Since we started with an arbitrary element q of our poset $\mathbb{P}$ and obtained $r \leq q$ with $r \in D$, we can conclude that D is dense in $\mathbb{P}$.

Since D is dense and G is $\mathbb{P}$-generic, it follows that $D \cap G$ is nonempty. If the intersection happens in the second set, then there exists a $q \in G$ such that $q \perp r$ for all $r \in E$, and we're done.

Otherwise, there exists $q \in G$ such that there exists $r \in E$ with $q \leq r$. Since G is closed upwards, it follows that $r \in E \cap G$. This proves (i).

To get (ii), let E be dense below p, and assume that $G \cap E = \emptyset$. As we've just proved, there must exist some $q \in G$ such that $q \perp r$ for all $r \in E$.

Let q' be a common strengthening of p and q. Since E is dense below p, there exists $r \in E$ such that $r \leq q' \leq q$. However, this is impossible, since we know that q is incompatible with every element of E. Contradiction! $\square$

6.5 Homework!

1. Prove that if $q \leq p$ and $p \Vdash \phi(\tau_1, \ldots, \tau_n)$, then $q \Vdash \phi(\tau_1, \ldots, \tau_n)$.
2. Look over our proof that $M[G]$ satisfies the axiom of separation. See if you can use a similar strategy to show that $M[G]$ satisfies the axiom of replacement. (Ask Susan if you need the statement of the axiom.)
3. This was kind of a tough day. Go over your notes. Find places where you're confused. Ask me questions.

7 Defining The Forcing Relation in $\mathscr{M}$

7.1 The "Forcing" Relation

Hold onto your hats. This is going to get pretty crazy.

(a) $p \Vdash_* (\tau_1 = \tau_2)$ if and only if

(i) For all $(\pi_1, s_1) \in \tau_1$, the set

$$\{q \in \mathbb{P} : (q \leq s_1) \Rightarrow (\exists (\pi_2, s_2) \in \tau_2 \text{ s.t. } ((q \leq s_2) \wedge (q \Vdash_* (\pi_1 = \pi_2))))\}$$

is dense below p.

(ii) For all $(\pi_2, s_2) \in \tau_2$, the set

$$\{q \in \mathbb{P} : (q \leq s_2) \Rightarrow (\exists (\pi_1, s_1) \in \tau_1 \text{ s.t. } ((q \leq s_1) \wedge (q \Vdash_* (\pi_1 = \pi_2))))\}$$

is dense below p.

(b) $p \Vdash_* (\tau_1 \in \tau_2)$ if and only if the set

$$\{q : \exists (\pi, s) \in \tau_2 \text{ such that } q \leq s \text{ and } q \Vdash_* (\pi = \tau_1)\}$$

is dense below p.

(c) $p \Vdash_* (\phi(\tau_1, \ldots, \tau_n) \wedge \psi(\tau_1, \ldots \tau_n))$ if and only if p "forces" both expressions.

(d) $p \Vdash_* (\neg\phi(\tau_1, \ldots, \tau_n))$ if and only if there is no $q \leq p$ with $q \Vdash_* \phi(\tau_1, \ldots, \tau_n)$.

(e) $p \Vdash_* \exists x(\phi(x, \tau_1, \ldots, \tau_n))$ if and only if the set

$$\{q : \exists \sigma \in M^{\mathbb{P}} \text{ such that } q \Vdash_* \phi(\sigma, \tau_1, \ldots, \tau_n)\}$$

is dense below p.

Let's unpack this a little bit. Condition (a) is far and away the hardest to read, and it's partially because we had to use insanely, unreadably compact notation to get it to fit nicely on a page.[25]

What condition (a), (i) says is that for any $(\pi_1, s_1) \in \tau_1$, a certain set[26] is dense below p. So if $p \in G$, some element of that big ugly set has to be in

[25] Or the chalk board, for that matter.

[26] A certain ugly, unreadable set.

G as well. So, working through carefuly, we know that if $p \in G$, then there exists some $q \in G$ satisfying... gak!

Right. Now let's address gak. If q is in this set, then $(q \leq s_1)$ implies that there exists $(\pi_2, s_2) \in \tau_2$ such that $q \leq s_2$ and $q \Vdash_* (\pi_1 = \pi_2)$. So we have two possibilities:

The first possibility is that there is some $q \in G$ with $q \leq s_1$, $q \leq s_2$, and $q \Vdash_* (\pi_1 = \pi_2)$, in which case $\pi_{1_G} \in \tau_{1_G}$, $\pi_{2_G} \in \tau_{2_G}$, and $\pi_{1_G} = \pi_{2_G}$. The second possibility is that there is no $q \leq p$ such that $q \leq s_1$, and so $s_1 \perp p$, which means that $\pi_{1_G} \notin \tau_{1_G}$.

So what (a)(i) is saying, when everything is put together, is that if p is an element of G, then $\tau_{1_G} \subseteq \tau_{2_G}$. As an exercise,[27] you should convince yourself that (a)(ii) says that if $p \in G$, then $\tau_{2_G} \subseteq \tau_{1_G}$, and that what (b) says is that if $p \in G$, then $\tau_{1_G} \subseteq \tau_{2_G}$.

This establishes that the $\Vdash_*$ relation means the same thing as the $\Vdash$ relation for atomic formulas. The expressions in (c), (d), and (e), allow us to build up formulas using the various logical connectors that we need. And (c) and (e) seem totally fine and strightforward. But then there's (d)...

7.2 Okay... So How About (d)?

This is the sneaky step. This says that if no q below p forces ϕ to be true, then $p \Vdash_* \neg\phi$. That means that unless there is some $q \in G$ with $q \Vdash_* \phi$, the sentence ϕ *cannot* be true in $M[G]$. So every single true statement in $M[G]$ must be forced to be true by some element of G.

This does not even remotely follow from our big-model definition of $\Vdash$, but you can make a reasonable intuitive argument for it. After all, we're building a universe $M[G]$ out of puzzle pieces that we get from $\mathbb{P}$. And if you're building a cat puzzle and you never encounter a partial image that looks like an ear, in the end your'e going to end up with a picture of an earless cat. So if $M[G]$ is going to satisfy ϕ, then it stands to reason that we should have some piece somewhere in $\mathbb{P}$ that says that ϕ will happen. Nice argument, but not particularly satisfying mathematically.

So let's take a really simple sentence: say $\tau_1 = \tau_2$. We know that if there exists $p \in G$ with $p \Vdash_* (\tau_1 = \tau_2)$, then $\tau_{1_G} = \tau_{2_G}$. Let's try to prove that the

[27] No really. It's a homework problem.

converse also holds:

Theorem: If $\tau_{1_G} = \tau_{2_G}$, then there exists $p \in G$ such that $p \Vdash_* (\tau_1 = \tau_2)$.

Proof. Since our model $\mathscr{M}$ is well-founded, we can induct on the maxium rank of the $\mathbb{P}$-names τ_1 and τ_2. If $\tau_1 = \tau_2 = \emptyset$, then $\tau_{1_G} = \tau_{2_G} = \emptyset$ for any filter G, and so we'll have $p \Vdash_* (\tau_1 = \tau_2)$ for all $p \in G$. Yay base case!

Now assume that $\tau_{1_G} = \tau_{2_G}$, and assume that the result holds for all $\mathbb{P}$-names of smaller rank. Define a set D, consisting of all $r \in \mathbb{P}$ satisfying one of the following three properties:

($\star$) $r \Vdash_* (\tau_1 = \tau_2)$.

(i′) There exists $(\pi_1, s_1) \in \tau_1$ such that $r \leq s_1$, and for any $(\pi_2, s_2) \in \tau_2$ and $q \in \mathbb{P}$, we have

$$((q \leq s_2) \text{ and } q \Vdash_* (\pi_1 = \pi_2)) \Rightarrow (q \perp r)$$

(ii′) There exists $(\pi_2, s_2) \in \tau_2$ such that $r \leq s_2$, and for any $(\pi_1, s_1) \in \tau_1$ and $q \in \mathbb{P}$, we have

$$((q \leq s_1) \text{ and } q \Vdash_* (\pi_1 = \pi_2)) \Rightarrow (q \perp r)$$

Claim 1: D is dense in $\mathbb{P}$.

To see that this is true, consider an arbitrary p. We need to show that there exists some $r \leq p$ satisfying ($\star$), (i′), or (ii′). If $p \Vdash_* (\tau_1 = \tau_2)$, then we're already done. So assume that $p \nVdash_* (\tau_1 = \tau_2)$. Then p fails to satisfy either (i) or (ii). Without loss of generality, let's say that p fails to satisfy (i). Now we need to find a negation for (i).

To say that (i) is not true means that there exists $(\pi_1, s_1) \in \tau_1$ such that the set

$$S = \{q \in \mathbb{P} : (q \leq s_1) \Rightarrow (\exists (\pi_2, s_2) \in \tau_2 \text{ s.t. } ((q \leq s_2) \wedge (q \Vdash_* (\pi_1 = \pi_2))))\}$$

is not dense below p. That is, there exists some $r \leq P$ such that for every $q \leq r$, $q \notin S$. Playing the negation game again, this says that for every $q \leq r$, we have $q \leq s_1$ and for all $(\pi_2, s_2) \in \tau_2$, either $(q \not\leq s_2)$ or $q \nVdash_* (\pi_1 = \pi_2)$.

Now we're going to show that this r that we've been talking about is actually an element of (i′). First of all, since $r \leq r$, we have $r \leq s_1$. Now suppose there exists some q compatible with r such that $q \leq s_2$ and $q \Vdash_* (\pi_1 = \pi_2)$. Then

their common strengthening q' satisfies $q \leq s_2$, $q \Vdash_* (\pi_1 = \pi_2)$, and $q \leq r$. Contradiction!

Ooph, so this shows that D is dense in $\mathbb{P}$. So G must intersect with D somewhere. Hopefully G intersects with D in an element that satisfies $(\star)$. Our next step is to prove that G *cannot* intersect with D in an element that satisfies (i′) or (ii′).

Claim: If r satisfies (i′) or (ii′), then it cannot belong to G.

The proof for (i′) and (ii′) is entirely analogous, so let's just do the proof for (i′). Suppose $r \in G$ and r satisfies (i′). Since $r \leq s_1$, we have $s_1 \in G$, so $\pi_{1_G} \in \tau_{1_G}$. Since $\tau_{1_G} = \tau_{2_G}$, this means that there must be some $(\pi_2, s_2) \in \tau_2$ such that $s_2 \in G$ and $\pi_{2_G} = \pi_{1_G}$.

By the inductive hypothesis,[28] there exists $p \in G$ such that $p \Vdash_* (\pi_1 = \pi_2)$. Since p and s_2 are both elements of G, they must have a common strengthening q. We know that $q \leq s_2$, and since $q \leq p$, we have $q \Vdash_* (\pi_1 = \pi_2)$. But since $q \in G$, we can't have $q \perp r$. Contradiction![29] □

[28] Since π_1 and π_2 are both $\mathbb{P}$-names of smaller rank.

[29] And congratulations. This is far and away the hardest proof we'll be doing in this class.

7.3 Homework!

1. Run yourself through the argument that if p satisfies the condition given in (a)(ii), then $\tau_{2_G} \subseteq \tau_{1_G}$. Then find a simliar arugment to convince yourself that if p satisfies the condition given in (b), $p \in G$ implies that $\tau_{1_G} \in \tau_{2_G}$.
2. An easier question than 1! Convince yourself that (c) and (e) properly define how the forcing relation should interact with $\wedge$ and $\exists$.
3. Show that if $\tau_{1_G} \in \tau_{2_G}$, then there exists $p \in G$ such that $p \Vdash_* (\tau_1 \in \tau_2)$. (Assume the corresponding result about the "=" relation from class today.)
4. If you have time, take another look at the "=" proof from class to get a better sense of what's going on.[30]
5. Convince yourself that the $\Vdash_*$ relation is the same as the $\Vdash$ relation for all formulas $\phi(\tau_1, \ldots, \tau_n)$.

[30]This is one of the toughest proofs we're doing in this class, so it's worth looking over. However, it's the result that we'll need in the later material, not the proof. So take a few days with this if you need to!

8 Finishing Off The Axioms And An Important Lemma

Last time, we talked through the proof that $\Vdash$ is definable in M. A part of that proof was to verify the definition of $p \Vdash_* \neg\phi$ by showing that if ϕ is true in G, then there is some q in G such that $q \Vdash \phi$. This proves the forcing theorem for us. Now we can knock out our three remaining set theory axioms!

8.1 Replacement

Essentially,[31] what replacement says is that the image of any function is a set. That is, for any set a, and for any tuple of variables $\overline{w}$ and any formula $\phi(x, y, \overline{w})$ such that for any set $x \in a$ there exists a unique y that makes $\phi(x, y, \overline{w})$ true, we have a set

$$\{y : \exists x \text{ such that } \phi(x, y, \overline{w})\}.$$

To prove that this holds in $M[G]$, we need to show that for any such formula $\phi(x, y, \overline{w})$ and for any $\sigma_G, \overline{\tau_G}$ such that for any $x \in \sigma_G$ there exists a unique y such that $\phi(x, y, \overline{\tau_G})$ is true in $M[G]$, the image of this "function" is also a set in $M[G]$. That is, we want to bulid the set

$$S = \{\mu_G : \pi_G \in \sigma_G, \phi(\pi_G, \mu_G, \overline{\tau}_G\}$$

Define a $\mathbb{P}$-name

$$\xi = \{(\mu, p) : \exists(\pi, s) \in \sigma \text{ s.t. } p \Vdash (\pi \in \sigma) \wedge \phi(\pi, \mu, \overline{\tau})\}$$

Clearly, every element of ξ_G is an element of S. We know that the elements of S will all be elements of ξ_G because if μ_G satisfies $\exists \pi_G \in \sigma_G$ with $\phi(\pi_G, \mu_G, \overline{\tau}_G)$, then some specific element $p \in \mathbb{P}$ forces it to happen.

[31] Formally, for any formula ϕ with appropriate free variables,

$$\forall a \forall \overline{w}(\forall x \in a \exists! y \phi(x, y, \overline{w}, a) \Rightarrow \exists b \forall x \in a \exists y \in b \phi(x, y, \overline{w}, a)).$$

So... yeah... have fun parsing that.

8.2 Powerset

The powerset axiom states that if we have a set x, then the collection of sets y such that

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

is also a set. Now we'll have to be a little careful here, because "y is the powerset of x" is *not* an absolute statement. What we want to prove is that if $\sigma_G \in M[G]$, we have

$$\{z \in M^{\mathbb{P}} : z \subseteq \sigma_G\} \in M[G].$$

Again, we're going to aim for a set that's too large, and use separation to cut it down to size. We'll define a $\mathbb{P}$-name ξ as follows. For each $\mathbb{P}$-name τ such that $\mathrm{dom}(\tau) \subseteq \mathrm{dom}(\sigma)$,[32], we throw $(\tau, \mathbb{1})$ into ξ.

Let $\mu \in M^{\mathbb{P}}$, and let $\mu_G \subseteq \sigma_G$. We wish to show that $\mu_G \in \xi_G$. Let

$$\tau = \{(\pi, p) : (\pi \in \mathrm{dom}(\sigma)) \wedge (p \Vdash (\pi \in \mu))\}.$$

Clearly, $\mathrm{dom}(\tau) \subseteq \mathrm{dom}(\sigma)$, so $(\tau, \mathbb{1}) \in \xi$, which means that $\tau_G \in \xi_G$. We claim that $\tau_G = \mu_G$.

We know that $\mu_G \subseteq \sigma_G$, so any element of μ_G takes the form π_G for some $\pi \in \mathrm{dom}(\sigma)$. Since $\pi_G \in \mu_G$, there must be some $p \in G$ such that $p \Vdash (\pi \in \mu)$. This means that $(\pi, p) \in \tau$. It follows that $x \in \tau_G$ for all $x \in \mu_G$, and so $\mu_G \subseteq \tau_G$.

Now, any element of τ_G takes the form π_G, where $(\pi, p) \in \tau$ for some $p \in G$ such that $p \Vdash (\pi \in \mu)$. It follows that $\pi_G \in \mu_G$, and so $\tau_G \subseteq \mu_G$. Thus $\mu_G = \tau_G$, and our proof is complete.

8.3 The Axiom of Choice

To prove that $\mathscr{M}[G]$ satisfies the axiom of choice, we'll use the well-ordering version of the axiom. So we will take $x = \sigma_G \in M[G]$, and try to prove that it can be well-ordered.

[32]Sorry, just introduced a new notation! By domτ, we mean the set consisting of first coordinates of ordered pairs in τ, just as if we think of a function as ordered pairs satisfying a certain special property, the domain is the first coordinate of those pairs.

Let $s = \text{dom}(\sigma)$. Since this set is in M, it can be well-ordered in M. In particular, there exists a bijection

$$f : \alpha \to s$$

from an ordinal α to s. This bijection can be expressed as a set of ordered pairs:

$$\{\gamma, \pi_\gamma) : \gamma \in \alpha\}$$

Notation: Given $\mathbb{P}$-names δ and μ, we will use the notation (δ, μ) for the $\mathbb{P}$-name whose interpretation is (δ_G, μ_G). We will build such a $\mathbb{P}$-name as an exercise in the homework.

We define a $\mathbb{P}$-name

$$\tau = \{((\check{\gamma}, \pi_\gamma), \mathbb{1}) : \gamma \in \alpha\}.$$

Its interpretation is given by

$$\tau_G = \{(\gamma, \pi_{\gamma_G}) : \gamma \in \alpha\}.$$

This is a function from α to some set δ_G satisfying $\delta_G \supseteq \sigma_G$. Since some of the elements in $\text{dom}(\sigma)$ may have the same interpretation in $\mathscr{M}[G]$, this may not be a bijection. However, we can use this function to build an injection $g : \sigma_G \to \alpha$. We simply define $g(\mu_G) = \min\{\gamma : \tau_G(\gamma) = \mu_G\}$. From this injection, we obtain a bijection between σ_G, and a subset of α. Since α is an ordinal, the image of this bijection is well-ordered, so we can "steal" this well-ordering to well-order σ_G.

8.4 Hooray!

We have now proven that if $\mathscr{M}$ is a CTM, $\mathbb{P}$ is a poset in $\mathscr{M}$, and G is a $\mathbb{P}$-generic filter over $\mathscr{M}$, then we can create a CTM $\mathscr{M}[G]$ that contains all elements of M, and also contains the filter G. Go team!

8.5 Forcing ¬CH With Finite Partial Functions

Definition: If I and J are sets, we use the notation $F_n(I, J)$ for the **finite partial functions** from I to J, functions defined on some finite subset of the elements of I with images in J.

We can think of $F_n(I, J)$ as a collection of puzzle pieces which could be used to build a complete function from I to J. Since the finite partial functions

can be constructed from the axioms of ZFC in M using only a finite amount of information for each one, it follows that whenever I and J are in M, the set $F_n(I, J)$ is also in M.

Lemma 1: Let M be a CTM, and let $\kappa \in M$ be an ordinal. Let $\mathbb{P} = F_n(\kappa \times \omega, 2)$. This is the set of finite partial functions whose domain is the set of ordered pairs (α, n), with $\alpha \in \kappa$ and $n \in \omega$, and whose range is the set $\{0, 1\}$. Let G be $\mathbb{P}$-generic over M. Then $M[G] \models (2^{\aleph_0} \geq |\kappa|)$.

You see where we're going with this, right? If we prove this lemma and we apply it to the case where $\kappa = \aleph_2$, the second uncountable cardinal, then we have $2_0^{\aleph} \geq \aleph_2 > \aleph_1$, and we've proved that the continuum is larger than $\aleph_1$. In fact, we could use this with any cardinal number to show that the continuum is as large as we could possibly want![33]

Proof. For each $(\alpha, n) \in (\kappa \times \omega)$, define a set

$$D_{(\alpha,n)} = \{p : (\alpha, n) \in \mathrm{dom}(p)\} \in M.$$

Clearly, $D_{(\alpha,n)}$ is dense in $\mathbb{P}$, so $G \cap D_{(\alpha,n)} \neq \emptyset$. If we let $g = \bigcup G \in M[G]$, then g will be a complete function from $\kappa \times \omega$ to 2. That is,

$$g : \kappa \times \omega \to 2.$$

For each $\alpha < \kappa$, let $f_\alpha : \omega \to 2$ be defined by

$$f_\alpha(n) = g(\alpha, n).$$

Then $\{f_\alpha : \alpha < \kappa\} \in M[G]$. If we can show that $f_\alpha \neq f_\beta$ for all $\alpha \neq \beta$ in κ, then we will have κ distinct functions from ω to 2. Since there are $2^{\aleph_0}$ maps from ω to 2, it will follow that $|\kappa| \leq 2^{\aleph_0}$.

So let's do that, then! For each $\alpha \neq \beta$ in κ, define a set

$$E_{\alpha,\beta} = \{p : \exists n \text{ with } (\alpha, n), (\beta, n) \in \mathrm{dom}(p) \text{ and } p(\alpha, n) \neq p(\beta, n)\}.$$

This set exists in our model M and is clearly dense. Thus $G \cap E_{\alpha,\beta} \neq \emptyset$. It follows that $f_\alpha \neq f_\beta$, and our proof is complete. □

[33] In theory. I'll explain the catch after we get through this proof.

8.6 The Catch

So! Have we proved it? Well... not exactly. See, here's the thing: we've got this cardinal κ. And maybe $\kappa = \omega_2$. At least, it's ω_2 in M. But "being a cardinal number" is one of those nasty properties that is not necessarily absolute. So it's possible that we accidentally added things that "collapsed" ω_2—things that allowed us to see that, in fact, κ is countable in $M[G]$. So we'll need a way to show that we've forced without collapsing any of our cardinal numbers.

Tomorrow we will prove that if $\mathscr{M} \models$"$\mathbb{P}$ is CCC," and G is a $\mathbb{P}$-generic filter over $\mathscr{M}$, then the cardinal numbers in $\mathscr{M}[G]$ are exactly the same as the cardinal numbers in $\mathscr{M}$.

8.7 Homework!

1. The property "is an ordinal number" is absolute, but the property "is a cardinal number" is not. Explain why!

2. Technically when we talk about the ordered pair (a, b), we're really talking about the set $\{\{a\}, \{a, b\}\}$.[34]

   Given two $\mathbb{P}$-names π and σ, construct a $\mathbb{P}$-name whose interpretation is (π_G, σ_G).

3. If κ is an ordinal, a map $f : S \to \kappa$ is called **cofinal** if for every $\gamma \in \kappa$, there exists $s \in S$ such that $f(s) \geq \gamma$.

   (a) Give an example of a cofinal map into $\omega + 1$. Can you find an example where S has the smallest cardinality possible?

   (b) Suppose λ is the smallest ordinal such that there exists a cofinal map $f : \lambda \to \kappa$. Prove that there also exists a *strictly increasing* cofinal map $f : \lambda \to \kappa$.

[34] The ordered pair (a, a) is represented by the set $\{\{a\}\}$.

9 How To Preserve Cardinals

9.1 A Couple of Relevant Definitions

Definition: Let $\mathbb{P}$ be a poset in M. We say that $\mathbb{P}$ **preserves cardinals**[35] if whenever G is $\mathbb{P}$-generic over M and $\beta \in M$ is an ordinal, we have

$$(M \models (\beta \text{ is a cardinal}) \Leftrightarrow (M[G] \models (\beta \text{ is a cardinal}).$$

We say that $\mathbb{P}$ **preserves cofinalities** if whenever β is a limit ordinal, the cofinality of β calculated in $M[G]$ is the same as the cofinality of β calculated in M.

Sorry... Cof-wha-huh?

"Recall"[36] that a subset s of an ordinal κ is called **cofinal** if for any $\alpha \in \kappa$, there exists $\beta \in s$ such that $\beta \geq \alpha$. A map $f : \alpha \to \beta$ is called **cofinal** if for any $\gamma \in \beta$, there exists $\delta \in \alpha$ such that $f(\delta) \geq \gamma$. That is, the image of f is cofinal in β.

The **cofinality** of an ordinal number β, denoted $\text{cof}(\beta)$, is defined to be the smallest ordinal number α such that there exists a cofinal map $f : \alpha \to \beta$. This is also the smallest cardinality of a cofinal set in β.

An ordinal κ is called "regular" if $\text{cof}(\kappa) = \kappa$. Otherwise it is called "singular." Any regular ordinal κ is a cardinal.[37] Otherwise, we could take the bijection from a smaller ordinal α and it would be a cofinal map into κ.

Not all cardinals are regular, but every successor cardinal is regular. Why, do you ask? Well! Take $\aleph_{\alpha+1}$. Take the limit of the sequence of $\aleph_\alpha$ elements in $\aleph_{\alpha+1}$. Each of these elements have cardinality less than or equal to $\aleph_\alpha$. Thus the cardinality of the limit, the union of these sets, is at most

$$\aleph_\alpha \times \aleph_\alpha = \aleph_\alpha < \aleph_{\alpha+1}.^{38}.$$

We always have $\text{cof}(\text{cof}(\gamma)) = \text{cof}(\gamma)$, and so any cofinality is a regular cardinal. If there were a smaller ordinal that could map into $\text{cof}(\gamma)$, then it would have been the cofinality of γ.

[35] Feed the birds tuppence a bag?

[36] It's funny, because we've never defined this!

[37] "Recall" that an ordinal number κ is a cardinal number if for any ordinal number α with $|\alpha| = |\kappa|$, we have $\alpha \geq \kappa$ as ordinals.

[38] Dude, you should totally see the LaTeXcode for that statement

Let's gather a couple more useful facts about cofinality.

Fact: If $\text{cof}(\beta) = \kappa$, then there exists a strictly increasing cofinal map from κ to β.

Proof. Exercise! □

Fact: For any ordinal γ we have $\text{cof}(\text{cof}(\gamma) = \text{cof}(\gamma)$

Proof. Otherwise, $\text{cof}(\text{cof}(\gamma)) = \delta < \text{cof}(\gamma)$. Thus we have two strictly increasing cofinal maps $f : \delta \to \text{cof}(\gamma)$ and $g : \text{cof}(\gamma) \to \gamma$. We claim that the composition $g \circ f$ is a cofinal map from δ to γ. Consider any $\alpha \in \gamma$. We know that there exists $\beta \in \text{cof}(\gamma)$ with $g(\beta) > \alpha$. We also know that there exists $\mu \in \delta$ such that $f(\mu) > \beta$. Thus we have

$$g \circ f(\mu) = g(f(\mu)) > g(\beta) > \alpha$$

This proves that $g \circ f$ is cofinal. □

A similar argument gives us:

Fact: If $f : \kappa \to \gamma$ is cofinal, then $\text{cof}(\kappa) = \text{cof}(\gamma)$.

Oh, okay... \end{Cof-wha-huh}

Our goal is to show that our poset of final partial functions preserves cardinals[39] We will accomplish this by showing that our poset is CCC, that CCC posets preserve cofinalities, and that posets that preserve cofinialities preserve cardinals. Ready? Set? Go!

9.2 The March To The End Of The Proof

Lemma 2: If $\mathbb{P}$ preserves cofinalities, then $\mathbb{P}$ preserves cardinals.

Proof. Notice that everything from ω on down works the way it does in the universe, no mather what CTM we're in, so we can limit ourselves to thinking about ordinals $\beta > \omega$. Assume that $\mathbb{P}$ preserves cofinalities, and let $\kappa \geq \omega$ be a regular cardinal in M. Then

$$\text{cof}(\kappa)^{M[G]} = \text{cof}(\kappa)^{M} = \kappa.$$

[39] Mmm... pickled cardinal!

Since κ is regular in $M[G]$, κ must be a cardinal of $M[G]$.

If κ is a singular cardinal in M, then κ is the limit of successor cardinals in M, which are regular in M. Thus in $M[G]$, κ is still the limit of regular cardinals, and hence a singular cardinal. □

Lemma 3: Suppose that whenever G is $\mathbb{P}$-generic over M and

$$M \models \text{“}\kappa \text{ is an uncountable regular cardinal.”}$$

we have $M[G] \models$“κ is regular.” Then $\mathbb{P}$ preserves cofinalities.

Proof. Assume that whenever κ is an uncountable regular cardinal in M, we know that κ is a regular cardinal in $M[G]$. Let $\gamma \in M$ be any limit ordinal, and let $M \models (\kappa = \text{cof}(\gamma))$. Clearly, we may also assume $\kappa > \omega$. There exists a strictly increasing function $f \in M$ such that f maps κ cofinally into γ.[40] By assumption,

$$M[G] \models (\text{cof}(\kappa) = \kappa).$$

Also, since $f \in M[G]$, it follows that

$$M[G] \models (\text{cof}(\kappa) = \text{cof}(\gamma)).^{41}$$

Since $M[G]$ believes that κ is regular, it follows that

$$M[G] \models \text{cof}(\gamma) = \kappa.$$

□

Lemma 4: Assume that $\mathbb{P} \in M$, and that

$$\mathscr{M} \models \mathbb{P} \text{ is CCC.}$$

Let A and B be elements of M, and let G be $\mathbb{P}$-generic over $\mathscr{M}$. Let $f \in \mathscr{M}[G]$ such that $f : A \to B$. Then there exists $F : A \to \mathscr{P}(B)$ such that

(i) $F \in M$.

(ii) $f(a) \in F(a)$ for all $a \in A$.

(iii) For all $a \in A$, $\mathscr{M} \models |F(a)| \leq \aleph_0$.

[40] Exercise!

[41] Exercise!

Proof. Proof delayed. □

Lemma 5: If $\mathbb{P} \in M$ and $\mathscr{M} \models$"$\mathbb{P}$ is CCC," then $\mathbb{P}$ preserves cofinalities.

Proof. Suppose $\mathbb{P}$ is CCC, but does not preserve cofinalities. Then there exists $\kappa \in M$ such that κ is a regular uncountable cardinal in $\mathscr{M}$, but κ is not regular in $\mathscr{M}[G]$.

Since κ is not regular in G, there exists a cofinal map $f : \alpha \to \kappa$ for some $\alpha < \kappa$.

Thus there exists $F : \alpha \to \mathscr{P}(\kappa)$ such that

(i) $F \in M$.

(ii) $f(\gamma) \in F(\gamma)$ for any $\gamma < \alpha$.

(iii) $M \models |F(\gamma)| \leq \aleph_0$ for all $\gamma < \alpha$.

$S = \bigcup_{\gamma \in \alpha} F(\gamma)$ an element of M. By (ii), S is cofinal. Computing in $\mathscr{M}$,

$$|S| = |\alpha| < \kappa.$$

Thus there is a cofinal set in $\mathscr{M}$ smaller than κ, contradicting our assumption that κ is regular in $\mathscr{M}$. Thus $\mathscr{M}$ must preserve cofinalities. □

Proof of Lemma 4. Suppose that $\mathscr{M} \models \mathbb{P}is$ CCC, and there exists $f : A \to B$ in $M[G]$. Then there is some $\mathbb{P}$-name τ such that $\tau_G = f$. Since f is a function from A to B, there exists some $p \in \mathbb{P}$ such that

$$p \Vdash \tau : \check{A} \to \check{B}$$

Define the set $F(a)$ to be

$$\{b \in B : \exists\ q \leq p \text{ with } q \Vdash \tau(\check{a}) = \check{b}\}$$

We know that $f(a) \in F(a)$, because some q must force $\tau(\check{a})$ to be equal to $f(a)$.

To show that $\mathscr{M}$ believes that $F(a)$ is countable, suppose the contrary. Then there are uncountably many b, and uncountably many q_b such that $q_b \Vdash \tau(\check{a}) = \check{b}$. But all of these q's would be pairwise incompatible with each other. Since $\mathscr{M}$ believes that $\mathbb{P}$ hs no uncountable antichains, this is impossible. □

9.3 Homework!

1. Prove that if $\text{cof}(\beta) = \kappa$, then there exists a strictly increasing cofinal map $f : \kappa \to \beta$.
2. Prove that if there exists a strictly increasing cofinal map $f : \kappa \to \gamma$, then $\text{cof}(\kappa) = \text{cof}(\gamma)$.

10 The Last Few Things

10.1 The Δ-System Lemma

Definition: A family $\mathscr{F}$ of finite sets is called a Δ-system with root R if whenever $A, B \in \mathscr{F}$ satisfy $A \neq B$, we have $A \cap B \in R$. (Note: We allow $R - \emptyset$.

The Δ-System Lemma: If $\mathscr{F}$ is an uncountable family of sets, then there exists an uncountable Δ-system $\mathscr{F}_0 \subseteq \mathscr{F}$.

Proof. Since $\mathscr{F}$ is uncountable, and the collection of possible cardinalities for elements of $\mathscr{F}$ is countable, there must be some uncountable set $\mathscr{F}' \subseteq \mathscr{F}$ satisfying $|A| = n$ for all $A \in \mathscr{F}'$.

The value of n can't be equal to zero, because then we would only have one set in $\mathscr{F}'$. If the value of n is 1, then $\mathscr{F}'$ consists of uncountably many one-element sets. Then for any $A, B \in \mathscr{F}$ with $A \neq B$, we have $A \cap B = \emptyset$.

Now assume that the value of n is greater than 1, and that we can find a Δ-system inside for any uncountable collection of sets of size $(n-1)$. We have two cases:

Case 1: There exists an element s that appears in uncountably many sets in $\mathscr{F}'$. In this case, we define

$$\mathscr{F}'' = \{A \in \mathscr{F}' : s \in A\}.$$

We can now ignore s, which is in the intersection of any pair of these sets, and find a delta-system in $\mathscr{F}'$ by our inductive hypothesis.

Case 2: Each element s appears in only countably many sets. In this case, we define A_0 to be any set. Then to define A_α for a particular countable ordinal α, we consider the set

$$S = \bigcup_{\gamma \in \alpha} A_\gamma.$$

Since this is a countable union of finite sets, this is a countable set. Now we define

$$T = \{A \in \mathscr{F}' : s \in S, s \cap A \neq \emptyset\}$$

Since there are countably many $s \in S$, and each appears in only countably many $A \in \mathscr{F}'$, there must be only countably many $A \in T$. Choose $A_\alpha \in \mathscr{F}'$ such that $A_\alpha \notin T$.

This process gives us a set $\{A_\alpha : \alpha \in \omega_1\}$ such that $A_\gamma \cap A_\beta = \emptyset$ for each $\gamma \neq \beta$ in ω_1. This set is a Δ-system with root $\emptyset$. $\square$

10.2 Proof That $F_n(\kappa \times \omega, 2)$ Is CCC

Lemma 6: $F_n(I, J)$ is CCC whenever J is countable.

Proof. Let S be an uncountable subset of $F_n(I, J)$. Since J is countable, there are only countably many possible finite partial functions defined on any particular finite domain $I' \subseteq I$. It follows that we can find an uncountable subset $S' \subseteq S$ with $\text{dom}(p) \neq \text{dom}(q)$ for any $p \neq q$ in S'.

The domains of the functions in S' give us an uncountable family of sets. Thus by the Δ-system lemma, there exists a subset $R \subseteq I$, and an uncountable subset S'' such that if $p, q \in S''$, then $\text{dom}(p) \cap \text{dom}(q) = R$.

There are only countably many ways to assign values for a function on the finite set R, and so there must be $p, q \in S''$ with $p(r) = q(r)$ for any $r \in R$. Thus p and q are compatible with each other.

It follows that no uncountable subset of $F_n(I, J)$ can be an antichain, so $\mathbb{P}$ is CCC. This finally allows us to conclude the following:

Theorem: The negation of CH is consistent with ZFC. $\square$

10.3 Forcing The Consistency of CH

Definition: The set of **countable partial functions** from a set I to a set J is given by

$$\{f : I' \to J \mid I' \subseteq I, |I| < \omega_1\}$$

We use the notation $F_n(I, J, \omega_1)$.

Lemma: Suppose that $\mathscr{M}$ believes

$$\mathbb{P} = F_n(\omega_1, 2^\omega, \omega_1).$$

If G is $\mathbb{P}$-generic over $\mathscr{M}$, then

$$\mathscr{M}[G] \models |(2^\omega)^{\mathscr{M}}| \leq |(\omega_1)^{\mathscr{M}}|$$

Proof. G intersects with the dense sets

$$D_\alpha = \{p : \alpha \in \mathrm{dom}(p)\}$$

for all $\alpha \in \omega_1$, and with the dense sets

$$D_r = \{p : r \in \mathrm{im}(p)\}$$

for all $r \in 2^\omega$. Thus G allows us to build a surjective function $g : \omega_1 \to 2^\omega$. $\square$

Of course, we don't know that either $(\omega_1)^{\mathscr{M}} = (\omega_1)^{\mathscr{M}[G]}$, or that $(2^\omega)^{\mathscr{M}} = (2^\omega)^{\mathscr{M}[G]}$. That's what we'll need to do next.

10.4 Chains And Functions in $\mathbb{P}$

Lemma: If $\mathbb{P} = F_n(\omega_1, 2^\omega, \omega_1)$, and

$$p_0 \geq p_1 \geq p_2 \geq p_3 \geq \ldots$$

is a countable descending chain in $\mathbb{P}$, then there exists $q \in \mathbb{P}$ with $q \leq p_n$ for all $n \in \omega$.

Proof. Define $q = \bigcup_{n\in\omega} p_n$ to be the function defined on all values that appear in some p_n, such that $q(s) = p_n(s)$ whenever both are defined. Since there are countably many p's, the domain of q is a countable union of countable sets, and thus $q \in \mathbb{P}$. Clearly, we also have $q \leq p_n$ for all $n \in \omega$. $\square$

Lemma: If $\mathscr{M} \models \mathbb{P} = F_n(\omega_1, 2^\omega, \omega_1)$, G is $\mathbb{P}$-generic over $\mathscr{M}$, and $f : A \to B$ is a function satisfying:

(i) $f \in M[G]$

(ii) $A, B \in M$

(iii) $\mathscr{M} \models |A| < |\omega_1|$ Then $f \in M$.

Proof. Since $f \in M[G]$, there exists τ such that $\tau_G = f$. Since $\mathscr{M}$ believes that A is countable, we can define an onto function $\phi : \omega \to A$ in M.

Because $\tau_G : A \to B$, there must be some $p \in \mathbb{P}$ satisfying

$$p \Vdash \tau : \check{A} \to \check{B}.$$

Because τ_G is defined on every value of A, there exist b_0 and $p_0 \leq p$ in G satisfying

$$p_0 \Vdash \tau(\check{\phi}(\check{0})) = \check{b}_0$$

Similarly, if p_n is already defined, we can find b_{n+1} and $p_{n+1} \leq p_n$ in G satisfying

$$p_{n+1} \Vdash \tau(\check{\phi}(n \check{+} 1)) = \check{b}_n.$$

By our previous lemma, there exists $q \in \mathbb{P}$ satisfying $q \leq p_n$ for each $n \in \omega$.

We define a function $g : A \to B$ by taking

$$g = \{(\phi(n), b_n) : n \in \omega, q \Vdash \tau(\check{\phi})(\check{n}) = \check{b}_n\}.$$

The function g can be defined in M, and for each $\phi(n)$ in A, we have

$$g(\phi(n)) = \tau_G(\phi(n)) = f(\phi(n)),$$

and so $g = f \in M$. □

10.5 The Final Details

Fact: If $\mathscr{M} \models (\mathbb{P} = F_n(\omega_1, 2^\omega, \omega_1))$ and G is $\mathbb{P}$-generic over $\mathscr{M}$, then

$$(\omega_1)^{\mathscr{M}} = (\omega_1)^{\mathscr{M}[G]}$$

Proof. Suppose otherwise. Then there exists some surjective map $f : \omega \to (\omega_1)^{\mathscr{M}}$ in the model $\mathscr{M}[G]$. However, ω is countable, so this would mean that f is also in M, contradicting the fact that $\mathscr{M}$ believes the image is ω_1. □

Fact: If $\mathscr{M} \models (\mathbb{P} = F_n(\omega_1, 2^\omega, \omega_1))$ and G is $\mathbb{P}$-generic over $\mathscr{M}$, then

$$(2^\omega)^{\mathscr{M}} = (2^\omega)^{\mathscr{M}[G]}$$

Proof. In either model, the set 2^ω will be the collection of functions from the set ω to the set 2. We can't lose such functions in passing from $\mathscr{M}$ to $\mathscr{M}[G]$, so the only possibility would be that we somehow obtain at least one function $f : \omega \to 2$ in $M[G]$ that is not in M. However, this is impossible, since ω is countable. □

Theorem: The continuum hypothesis is consistent with ZFC.

10.6 The ZFC Axioms

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

Union: $\forall z \exists y \forall x(x \in y \Leftrightarrow \exists u(x \in u \wedge u \in z))$

Powerset: $\forall z \exists y \forall x(x \in y \Leftrightarrow (\forall w(w \in x) \Rightarrow (w \in z))$

Replacement: Given a formula $\phi(x, y)$,

$$\forall u \forall v \forall w(\phi(u, v) \wedge \phi(u, w) \Rightarrow (v = w))$$
$$\Rightarrow$$
$$\forall z \exists y \forall v(v \in y \Leftrightarrow (\exists u(u \in z) \wedge \phi(u, v)))$$

Infinity: $\exists x((\emptyset \in x) \wedge \forall y((y \in x) \Rightarrow (y \cup \{y\}) \in x)$

Foundation: $\forall x \exists y((y \in x) \wedge \forall z((z \in y) \Rightarrow \neg(z \in x)))$

Choice: Erf totally ran out of time before TAU. New handout tomorrow. Sorry!!!