

## CH - Pizza Seminar 2/1/08

### 1 Introduction

The continuum hypothesis (CH) is the following:

**Definition 1.1.** Every infinite subset  $X \subseteq \mathbb{R}$  either has the cardinality of  $\mathbb{N}$  or has the cardinality of  $\mathbb{R}$ .

Our goal today is to use a method called forcing to hand wave the following:

**Theorem 1.1.** *The continuum hypothesis is independent of the axioms of ZFC. That is, if we assume the axioms of ZFC, we can neither prove nor disprove CH.*

When stated like this, it's clear that to prove something is independent requires two parts - proving it can't be proven and proving it can't be disproven.

The question about whether or not CH is true or false has been around since Cantor's day, and was the first Millennium problem offered by Hilbert in his famous address. Partial progress was made in the 1930's when Godel showed that, given the axioms of ZFC, we cannot disprove CH. The converse, that we cannot prove CH either, wasn't shown until the 1960's, when Paul Cohen, an analyst, developed a new method known as forcing. Forcing has since grown into the most common and powerful technique for proving general independence results.

Before moving onto what exactly ZFC is, I want to work with a set of simpler axioms and demonstrate exactly what is meant by independent.

**Definition 1.2.** The group axioms are:

1.  $\forall a, b, c, (ab)c = a(bc)$
2.  $\exists e$  such that  $\forall a, ae = ea = a$ .
3.  $\forall a \exists b$  such that  $ab = ba = e$ .

**Definition 1.3.** A group  $G$  is a set with binary operation satisfying the group axioms

Loosely speaking, a group is a *model* of the axioms. In other words, it's a set together with interpretations (of constants, relations, functions, etc) such that under that particular interpretation, all the "group axioms" are satisfied.

Here is an example of a statement that's NOT independent of the group axioms:

There is a non-identity  $b$  such that  $ab = ba = a$  for all  $a$  (In other words, the identity is unique). In fact, it's false

Here is a statement that is:

$$\forall a, b, ab = ba.$$

So, what do I mean by independent? Formally, I mean there is no way to start with the group axioms, and using normal laws of deduction, arrive at the above statement. However, it's much easier than that. Is there an example (a model) of a group which satisfies this statement? Sure,  $G = \frac{\mathbb{Z}}{2\mathbb{Z}}$  does it. Thus, we certainly can't prove a group DOESN'T satisfies it, because we have one that does. Similarly, is there an example of a group which doesn't satisfy the statement? Sure, let  $G = S_3$ . Thus, we certainly can't prove a group must be commutative, since we have an example of a noncommutative group.

(For the person who finds this too informal, the driving force behind this is the Godel Completeness theorem - A collection of axioms is consistent iff it has a model. Here, the group of axioms we want to be consistent is the the group axioms + the extra, as well as the group axioms + the negation of the extra).

This is the basic idea behind all independence results. Moving towards showing something is independent of the axioms of ZFC, let's first briefly talk about what those axioms are.

**Definition 1.4.** ZF is all the following axioms.

1. There is a set. In fact, there is an infinite set
2. If  $X$  and  $Y$  are sets, so are  $\{X, Y\}, P(X), \bigcup X, X \times Y, etc.$
3. If  $X$  is a set and  $\phi$  is a formula, then  $Y = \{x \in X : \phi(x)\}$  is also a set
4. If  $X$  is a set and  $f$  is a function, then  $f(X)$  is a set.
5. There is no infinite decreasing sequence  $X_0 \ni X_1 \ni X_2 \dots$

ZFC is ZF +

6. Every set can be well ordered

So, following our above example, to show the independence of CH from ZFC, we need only find 2 examples - one of a set satisfying all of the above axioms, where CH fails, and another one a set satisfying all of the above axioms, where CH is true.

We now run into our first difficulty:

**Theorem 1.2.** (*Godel incompleteness*) *If we work in a system satisfying ZFC, then we cannot produce a model of ZFC. In fact, we're not even sure if ZFC has models at all.*

The problem of whether or not there are models at all is an easy one. Again, according to Godel, ZFC is consistent iff it has a model. Since many believe ZFC the foundation of all mathematics, we're willing to believe it's consistent. Thus, it has a model.

So, now we know it has a model. Does that model satisfy CH? Who knows? Thus, it won't be as easy as just coming up with a model out of thin air. So, what do we do? The idea is that we'll start with any model at all and show how to enlarge it in such a way that the bigger model satisfies CH (or doesn't). It's important that we do this without using any structure of the smaller model because, well, we know nothing about the structure of the smaller model.

Let's take another cue from group theory... Suppose  $H$  is a subgroup in some much larger group  $G$ . Further, assume  $H$  is commutative within itself, and maximal in this sense (if  $a$  commutes with  $H$ , then  $a$  is in  $H$ ), but that  $G$  is not. Then, there is some  $a \in G$  and some  $b \in H$  with  $ab \neq ba$ . Let  $K =$  smallest group containing  $H$  and  $a$ . Then  $K$  is clearly non commutative.

The point is, we can start with a commutative thing, add something (and maybe add a ton to make all the axioms still be satisfied), and end up with something noncommutative.

We'll do the same thing with ZFC, though we'll, of course run into a few more difficulties.

More generally, here's what we'll do: First, we'll start with ANY model whatsoever and show how to extend it to a bigger model where CH holds. Then we'll do the same, except extend it to one where CH fails.

(Draw picture with  $M, V$ , and  $G$ ).

## 2 The idea of forcing

The big picture is as follows. In the background is a theorem by Lowenheim and Skolem (downward) which states that if you hand me any model at all, I can find a countable (transitive) submodel which is elementary equivalent. This just means that from the point of view of logic, they're identical - a (first order) statement is true in the big model iff it's true in the small model.

I want to point out how strange this is. In my model, I have something I call the real numbers. I can prove that the collection of these is uncountable. What I'm REALLY proving is that if there is a bijection between what I call the real numbers and what I call the natural numbers, then it doesn't live in model. HOWEVER- ACCORDING TO LOWENHEIM SKOLEM, I can assume that there is in fact such a bijection.

So, here's how it works. We mere mortals get our hands on our universe,

called  $M$ , a model of ZFC. Even though it doesn't look countable to us (it has every real number in it), there is someone bigger than us (God?) who DOES have a bijection between our model and  $\mathbb{N}$ , and further, has his own model of ZFC, called  $V$ , of which we are a submodel.

Now, we mere mortals have something called the Rasiowa-Sikorski Lemma, which basically tells us that if a partial order is countable, then there's a particularly nice subset of it called a (generic) filter. So, we know that according to God, a generic filter exists. We can also prove that under some fairly weak hypothesis on our partial order, the generic filter CAN'T be a part of our model. Thus, we can use the existence of the filter to "enlarge" our own model. That is, for any filter  $G$ , we can construct "the smallest model containing all of us, plus the filter", denoted  $M[G]$ . Further, we mortals can prove facts like "if  $p \in G$ , then the following statement is true" Note however, that in general, we have NO idea if a given  $p \in G$ . That said, one can sometimes still prove things like "For any  $G$  at all, the following is true". This will be enough to demonstrate the independence of CH.

Now we move onto a few details.

### 3 A quick word on cardinals

The ordinal numbers are best thought of as canonical representatives of the isomorphism classes of well ordered sets. In other words, for any given well ordered set, there is a unique ordinal number which is order isomorphic to the given set. The strange fact is that the collection of ordinal numbers (while not a set) is well ordered (any subSET of ordinal numbers has a least element). Cardinal numbers are particular ordinal numbers (VERY few ordinal numbers are cardinal numbers). As such, the collection of Cardinal numbers (still too big to be a set) is well ordered.

**Definition 3.1.**  $\omega_0 = \omega = |\mathbb{N}| = \text{"}\mathbb{N}\text{"}$  is first infinite cardinal number. It is countable. The rest of the infinite cardinal numbers will be labeled  $\omega_1, \omega_2, \dots$ .  $\omega_1$  is uncountable, and the least such cardinal with this property. In this language, the continuum hypothesis can be restated as  $|\mathbb{R}| = \omega_1$ . Notice that  $|P(\omega)| = |\mathbb{R}| = |\{f : \omega \rightarrow \{0, 1\}\}|$ . Let  $2^\omega$  denote  $\{f : \omega \rightarrow \{0, 1\}\}$ .

### 4 moving on to a few details

**Definition 4.1.**  $Func_{\omega_\alpha}(X, Y) = \{f : A \subseteq X \rightarrow Y : |A| < \omega_\alpha\}$ .  $Func(X, Y) = Func_\omega(X, Y)$ . We order Func by reverse inclusion, i.e. for  $f, g \in Func$ ,  $f \leq g$  iff  $g \subseteq f$ . That is,  $f \leq g$  iff  $f$  extends  $g$ .

**Definition 4.2.** Given a partially ordered set  $\mathbb{P}$ , a subset  $D \subseteq \mathbb{P}$  is dense if  $\forall p \in \mathbb{P}, \exists d \in D$  with  $d \leq p$ . Note that this may not be the usual notion of density you're used to!

**Definition 4.3.**  $G \subseteq \text{Func}_{\omega_\alpha}(X, Y)$  is called a filter if, if  $f, g \in G$ , then  $\exists h \in G$  with  $h \leq f$  and  $h \leq g$ . In otherwords, any two functions in  $G$  are compatible. Also, we require that if  $f \in G$  and  $g \in \text{Func}$  with  $f \leq g$ , then  $g \in G$ . In otherwords, anything which provides less, but still compatible information with what already in  $G$  is thrown into  $G$ . In particular, we can think of  $G$  as a map from a subset  $A = \bigcup_{f \in G} \text{dom}(f) \subseteq X$  to  $Y$ .

**Theorem 4.1.** (*Risiowa-Sikorski*) If  $D = \{D_n : n \in \omega\}$  is a countable collection of dense sets, then there exists a filter  $G$  such that  $G \cap D_n \neq \emptyset$  for each  $n$ .

So, who cares? Lets give an example.

Consider  $\text{Func}(\mathbb{N}, Y)$ . Let  $D_n = \{p \in \text{Func} : n \in \text{dom}(p)\}$ . This is dense because if you hand a function  $g$  with  $n$  in it's domain, then it's already in the dense set. If  $n$  isn't in it's domain, arbitrarily extend  $g$  to have  $n$  in it's domain. I.e., let  $h$  be defined on  $\text{dom}(g) \cup n$  with  $h(x) = g(x)$  for  $x$  in  $\text{dom}(g)$  and  $h(n) = \text{whatever}$ . Then  $\text{dom}(h)$  is still finite, and  $h$  extends  $g$  so  $h \leq g$  and  $h$  is in  $D_n$ . Then, if  $G$  intersects it, then  $\exists g \in G$  with  $n \in \text{dom}(g)$ , so  $n \in \text{dom}(G)$ . Doing this for all  $n$  shows  $G$  is a map from all of  $\mathbb{N}$ , even though it's built out of functions which have only finite domains.

What I want to remind you of is the following. We starting with a ground model  $M$ , and a partially ordered set  $\text{Func}$  in  $M$ . We use Lowenheim-Skolem and Risiawa-Sikorski to get our hands on a filter  $G \subseteq \text{Func}$ , with  $G \notin M$ . We then get a new model  $M[G]$  formed as the least model containing all of  $M$  and  $G$ . But  $G$  is a function, so we can use it to witness bijections, or things like that.

However, we have to be careful of one HUGE possibility: collapsing cardinals.

To see the problem, let me illustrate with one example. In our model  $M$ , we think we have all of set theory. In particular, we have something we call  $\omega$  and something we call  $\omega_1$ . All this means, to us, is that we can check that  $\omega$  and  $\omega_1$  are cardinal numbers (whatever that really means) and further, we can find injections from  $\omega$  to  $\omega_1$ , but we have no surjections...IN OUR MODEL. So now, we get  $G$  added to our model, but the smallest model containing  $M$  and  $G$  might be huge - we may end up throwing all sorts of stuff in. It's possible that we throw in a surjection from  $\omega$  to  $\omega_1$ . In particular, what we used to call  $\omega_1$  is no longer  $\omega_1$  in  $M[G]$ , though in  $M[G]$  will have some new object which has all the defining properties of  $\omega_1$ .

It is a fundamental, nontrivial fact, that for the *Funcs* we'll be using, no matter what  $G$  we have, the cardinal numbers don't collapse. In other words,  $\omega_1$  in  $M$  is the same set as  $\omega_1$  in  $M[G]$ , and similarly for  $\omega_2$ , etc.

## 5 ZFC + not CH

Now, the really cool part is the Lowenheim-Skolem theorem allows us to think about ANY collection of dense sets as countable - this will give us a ton of power (though we'll have to be a bit careful)

That said, we're ready for half the result:

**Theorem 5.1.** *If ZFC is consistent (i.e., it has a model), then there is a model of ZFC in which CH fails. In particular, starting with ZFC, we can never prove CH is true.*

*Proof.* We will actually show that in the promised model,  $|\mathbb{R}| = |2^\omega| \geq \omega_2 > \omega_1$ . To that end, let  $\mathbb{P} = \text{Func}(\omega_2 \times \omega, \{0, 1\})$ .

Let  $D_{\beta,n} = \{p \in \mathbb{P} : (\beta, n) \in \text{dom}(p)\}$ . By an argument analogous to the one above, these are dense. According to Lowenheim-Skolem, since our own model is countable, so is this  $\omega_2$  thing, at least as it's seen by God. Thus, all of these  $D$ 's form a countable collection of dense sets.

Now, let  $E_{\alpha,\beta} = \{p \in \mathbb{P} : \exists n \in \mathbb{N} \text{ such that } p(\alpha, n) \neq p(\beta, n)\}$ . This is clearly dense as we can always find  $n$  such that  $p$  isn't defined on  $(\alpha, n)$  or  $(\beta, n)$  and define it there, one with value 0 and the other with value 1.

Thus,  $\{D_{\beta,n}, E_{\alpha,\beta}\}$  is a COUNTABLE collection of dense sets, so we get a filter  $G$  which intersects them all. Thinking of  $G$  as a function, we notice that since  $G$  intersects all the  $D_{\beta,n}$ ,  $\text{dom}(G) = \omega_2 \times \omega$ . Further, since  $G$  intersects all the  $E_{\alpha,\beta}$ , we have that for each  $\alpha, \beta$ , there is an  $n$  such that  $G(\alpha, n) \neq G(\beta, n)$ . Now, let  $g_\alpha(n) = G(\alpha, n)$ . Then clearly there are  $\omega_2$  of the  $g_\alpha$ 's. Further, they are all different by the previous argument. Thus, we've created  $\omega_2$  maps from  $\mathbb{N} \rightarrow \{0, 1\}$ . In other words,  $|\mathbb{R}| = |2^\omega| \geq \omega_2 > \omega_1$ . Thus, in this bigger model (which includes  $G$ ), CH fails.  $\square$

## 6 ZFC + CH

This one's actually much harder - not in principle, but in the details. The most important detail is as follows:

**Lemma 6.1.** *For  $\text{Func}_{\omega_1}(\omega_1 \times \omega, \{0, 1\})$ , if  $G$  is any filter and  $f : \omega \rightarrow \{0, 1\}$  is in  $M[G]$ , then  $f \in M$ . In other words, we don't add any new functions from  $\omega$  to  $\{0, 1\}$  when we move to a bigger model.*

**Theorem 6.2.** *If ZFC is consistent (i.e. it has a model), then there is a model of ZFC in which CH holds true. In particular, starting with ZFC, we can never disprove CH.*

*Proof.* Let  $\mathbb{P} = \text{Func}_{\omega_1}(\omega_1 \times \omega, \{0, 1\})$ . Again, we can choose dense sets which force a filter  $G$  to have  $\omega_1 \times \omega$  as its domain. Now, for any  $g : \omega \rightarrow \{0, 1\}$  with  $g \in M$ , let  $D_g = \{p \in \mathbb{P} : \exists \alpha \text{ such that } \{\alpha\} \times \omega \in \text{dom}(p) \text{ and } p(\alpha, n) = g(n) \forall n\}$ . To see that this is dense, notice that for any  $p \in \text{PO}$ , there is some  $\alpha$  such that  $\{\alpha\} \times \omega \cap \text{dom}(p) = \emptyset$ . Extend  $p$  by defining it on  $(\alpha, n)$  to agree with  $g$ . We'll come back to these in a second.

Now, let  $g_\alpha(n) = G(\alpha, n)$  and let  $A = \{g_\alpha\}$ . Then clearly  $|A| = \omega_1$ . I claim that  $A = 2^\omega$ , as seen by  $M[G]$ . This will establish that in  $M[G]$ ,  $|2^\omega| = |A| = \omega_1$ .

To prove that  $A = 2^\omega$  as seen by  $M[G]$ , notice that  $A$  is a collection of functions from  $\omega$  to  $\{0, 1\}$ , so  $A \subseteq 2^\omega$ . To see the converse, let  $g \in 2^\omega$  with  $g \in M[G]$ . Then by the above lemma,  $g \in M$ . Thus, we constructed a dense set  $D_g$  that  $G$  intersects. Thus,  $\exists \alpha$  such that  $G(\alpha, n) = g(n)$  for all  $n$ . But then  $g_\alpha = G(\alpha, n) = g$ , and  $g_\alpha \in A$ , so that  $g \in A$ .

□