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

14 Independence of CH

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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