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

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

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

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

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

Now define a "curried" version of F,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

is uncountable).

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

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

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

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

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

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

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

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

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