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

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

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

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

We wish to show that P is not an antichain.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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