Lecture 25: Independence of CH, part VI

April 22, 2009

Remark. We now return to finish the proof that $M[G]$ is a ctm.

Proof.

- Powerset. Let $\sigma_G \in M[G]$. We wish to construct some $\rho \in M^{\mathbb{P}}$ such that

  $$\forall x. x \subseteq \sigma_G \Rightarrow x \in \rho_G.$$

  This suffices, because once we have obtained a covering of the power set in this manner, we can use Separation to cut out the exact power set.

  To this end, let

  $$S = \{ \tau \in M^{\mathbb{P}} \mid \mathrm{dom}(\tau) \subseteq \mathrm{dom}(\sigma) \}.$$

  We note that $S \in M$, since it is equal to $[\mathcal{P}(\mathrm{dom}(\sigma) \times \mathbb{P})]^M$, and $\mathcal{P}(\mathrm{dom}(\sigma) \times \mathbb{P})$ exists in M since it is a ctm.

  Now let $\rho = S \times \{1_{\mathbb{P}}\}$. We claim that this is the desired ρ. To see this, suppose $\mu \in M^{\mathbb{P}}$ and $\mu_G \subseteq \sigma_G$; we must show that $\mu_G \in \rho_G$. Let

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

  We note that $\tau \in M$ by definability of forcing; also, τ has the form of a $\mathbb{P}$-name, so $\tau \in M^{\mathbb{P}}$. Then by definition of S, it is easy to see that $\tau \in S$. Therefore, $\tau_G \in \rho_G$.

  To complete the proof, we claim that $\tau_G = \mu_G$.

  - ($\mu_G \subseteq \tau_G$). Let $y \in \mu_G$. Since $\mu_G \subseteq \sigma_G$, there must be some $\pi \in \mathrm{dom}(\sigma)$ for which $y = \pi_G \in \sigma_G$. Therefore, by Truth, there is some $p \in G$ for which $p \Vdash \pi \in \mu$. So $\langle \pi, p \rangle \in \tau$ by definition, and hence $y = \pi_G \in \tau_G$ (since $p \in G$).
  - ($\tau_G \subseteq \mu_G$). Suppose $y \in \tau_G$. Then $y = \pi_G$ for some π with $\langle \pi, p \rangle \in \tau$, $p \in G$, and $p \Vdash \pi \in \mu$. So, by definition of forcing, $y = \pi_G \in \mu_G$.

- Choice. We first give the following alternate formulation of the well-ordering principle:

  $$\forall x. \exists f. \exists \alpha \in Ord. \, \mathrm{dom}(f) = \alpha \wedge x \subseteq \mathrm{rng}\, f.$$

  Some thought should show that this is equivalent to the familiar version of the well-ordering principle; given a set x, if we have a function f postulated by the above axiom, then we can use f to construct a well-ordering of x: put the elements of x in order according to the least β such that $f(\beta)$ yields them.

  Fix $x = \sigma_G$. Since M satisfies Choice, there is some well-ordering π of the elements of $\mathrm{dom}(\sigma)$:

  $$\mathrm{dom}(\sigma) = \{ \pi_\gamma \mid \gamma < \alpha \}$$

where $Ord(\alpha)$ and the function $\pi_{(-)} \in M$. π is a well-ordering of the domain of σ, which consists of names of elements of x (possibly plus some extra names). It is not hard to see that we can use a well-ordering of the names of elements of x to construct a well-ordering of x, as follows.

Let $\tau = \{\, \dot{\langle \dot{\gamma}, \pi_\gamma \rangle} \mid \gamma < \alpha \,\} \times \{1_{\mathbb{P}}\}$, where $\dot{\langle x, y \rangle}$ denotes the name for which $\dot{\langle x, y \rangle}_G = \langle x_G, y_G \rangle$. $\tau \in M^{\mathbb{P}}$ since M is a ctm. Moreover,

$$\tau_G = \{\, \langle \gamma, (\pi_\gamma)_G \rangle \mid \gamma < \alpha \,\}.$$

So τ_G is a function with domain α and $\sigma_G \subseteq \operatorname{rng} \tau_G$, as desired. ∎

Remark. Hence, $M[G]$ is a ctm; putting this result together with previous results, we have now shown (modulo the proofs of Truth and Definability) that there is a G for which

$$M[G] \models ZFC + \neg CH,$$

and therefore that CH is formally independent of ZFC!

15 Ramsey cardinals

Remark. And now, for something completely different! We will now attempt to show that

$$ZFC + Q \vdash V \neq L,$$

where Q is a large cardinal axiom. But first, Ramsey's Theorem!

Definition 15.1. For any set κ, we introduce the notation

$$[\kappa]^n = \{\, x \subseteq \kappa \mid \operatorname{card}(x) = n \,\},$$

that is, the collection of n-element subsets of κ. While this definition makes sense for any cardinal n, we will only use it for $n \in \omega$.

Definition 15.2. For any cardinals κ and λ, we define the relation

$$\kappa \to (\lambda)^n_\mu$$

to hold iff for every function $f : [\kappa]^n \to \mu$, there exists a set x such that

- $x \subseteq \kappa$,
- $\operatorname{card}(x) = \lambda$, and
- $f \restriction [x]^n$ is constant.

Remark. $f : [\kappa]^n \to \mu$ can be seen as a labeling of the n-element subsets of κ, using labels from μ. For example, if $n = 2$, such an f can be thought of as an edge coloring of the complete graph on κ nodes, using μ colors. If $\kappa \to (\lambda)^2_\mu$ holds, it means that we can find a subset of nodes of size λ which induces a monochromatically colored complete subgraph.

Theorem 15.3 (Ramsey's Theorem)**.** $\omega \to (\omega)^n_m$ *for all* $n, m \in \omega$.

Remark. This seems somewhat surprising! But it is true. In the finite case, it is famously true that for any $l \in \omega$, there exists some $k \in \omega$ such that $k \to (l)^2_2$, but the growth rate of the smallest such k with respect to l is astronomical (and unknown). Note famous quote by Erdős regarding this function and hostile aliens.

Proof. We will only prove the case for $\mu = n = 2$; it should be straightforward to see how to generalize the proof.

Let $f : [\omega]^2 \to \{0, 1\}$. We wish to construct a set $X \subseteq \omega$ of size ω for which $f \restriction [X]^2$ is constant. We mutually construct three sequences a_i, b_i, and X_i as follows:

$$\begin{aligned} X_0 &= \omega \\ a_0 &= 0 \\ X_{i+1} &= \{\, n \in X_i \mid f(\{a_i, n\}) = b_i \,\} && b_i \in \{0,1\} \text{ such that } X_{i+1} \text{ is infinite} \\ a_{i+1} &= \text{least } n \in X_{i+1} \text{ such that } n > a_i \end{aligned}$$

Note that we can always pick an appropriate b_i by an infinite version of the pigeonhole principle.

Again by the pigeonhole principle, either infinitely many $b_i = 0$, or infinitely many $b_i = 1$. So we may choose $X = \{\, a_i \mid b_i = b \,\}$, for whichever value of b makes X infinite (note that all the a_i are distinct since we chose them to form an increasing sequence).

We claim that $f \restriction [X]^2$ is constantly b. Let $a_i, a_j \in X$, and suppose, without loss of generality, that $j < k$. We know that $a_k \in X_k$; but since the X_i form a decreasing chain, $a_k \in X_{j+1}$ as well. But then by definition, $f(\{a_j, a_k\}) = b_j = b$. ∎