

Using the Δ -system Lemma we can prove Lemma 5.7.

Proof. We work in M , where \mathbb{P} was defined as all finite partial functions from $\omega \times \omega_2$ into 2. In fact let us prove something more general. Let I be an arbitrary set, and J an countable arbitrary set, and let $\text{Fn}(I, J)$ denote the set of all finite partial functions from I into J . We will show that $\text{Fn}(I, J)$ has the ccc.

Let X be an uncountable subset of $\text{Fn}(I, J)$. If we can find distinct p, q in X which are compatible then we will have shown that $\text{Fn}(I, J)$ is ccc. To do this, let $D = \{\text{dom}(p) : p \in X\}$.

There are two possibilities to consider. First suppose that D is countable; each $\text{dom}(p)$ is finite so the set $A = \bigcup D$ is a countable subset of I . There are only countably many possible finite subsets of A while X is uncountable. Thus there are two distinct p and q with $\text{dom}(p) = \text{dom}(q)$. Since p and q are distinct, they must disagree on some point of their domain and hence they are incompatible as we wanted.

The other possibility is that D is uncountable. Then D is an uncountable collection of finite sets and so by the Δ -system Lemma we can find $E \subseteq D$ which is uncountable and such that E is Δ -system with root r . Let $Y = \{p \in X : \text{dom}(p) \in E\}$; Y is uncountable.

If p belongs to Y , then $r \subseteq \text{dom}(p)$. Consider $p \upharpoonright r$; since J is countable there are only countably many possibilities for this function. As Y is uncountable then there must be distinct p, q in Y for which $p \upharpoonright r = q \upharpoonright r$. Since p, q are in Y , $\text{dom}(p)$ and $\text{dom}(q)$ are in E , and so $\text{dom}(p) \cap \text{dom}(q) = r$. It follows that $p \cup q$ is a well-defined function, so that p and q are indeed compatible. \square

Now that we have proved that \mathbb{P} is ccc let us see how we can take advantage of that fact in order to get that \mathbb{P} preserves cardinals. The following lemma is crucial.

Lemma 5.10. *Suppose $\mathbb{Q} \in M$ is ccc (within M), and let $A, B \in M$. Let G be \mathbb{Q} -generic, and let $f \in M[G]$ with $f : A \rightarrow B$. Then there is a function $F : A \rightarrow B$ such that $F \in M$, $f(a) \in F(a)$ for each $a \in A$, and for each $a \in A$ $F(a)$ is countable in M .*

Proof. Since f is in $M[G]$, there is a $\tau \in M^{\mathbb{Q}}$ such that $\tau[G] = f$. By Forcing Theorem A there is some $p \in G$ such that $p \Vdash \tau : \dot{A} \rightarrow \dot{B}$. We define $F : A \rightarrow B$ by setting

$$F(a) = \{b \in B : (\exists q \leq p) q \Vdash \tau(a) = b\}.$$

We claim that F is as desired.

Claim 1. $F \in M$.

Proof. This is because F is defined using absolute concepts on objects in M ; that \Vdash is absolute is by Forcing Theorem B. \square

Claim 2. For each $a \in A$, $f(a) \in F(a)$.

Proof. Suppose $f(a) = b$. Since $f \in M[G]$, $M[G] \models f(a) = b$. Thus there is $r \in G$ such that $r \Vdash \tau(a) = b$. Since both r and p belong to G they are compatible. Get $q \leq r, p$. Then $q \Vdash \tau(a) = b$ as well. Hence $b \in F(a)$ by definition. \square

Claim 3. For each $a \in A$, $F(a)$ is countable.

Proof. We work in M . For each $b \in F(a)$ there is by definition a $q_b \leq p$ such that $q_b \Vdash \tau(a) = b$. Notice that if $b \neq c$ then q_b and q_c are incompatible. For if $q \leq q_b, q_c$ then we would have both $q \Vdash \tau(a) = b$ and $q \Vdash \tau(a) = c$. But $q \leq p$, and $p \Vdash$ “ τ is a function” and so that is impossible. Thus $\{q_b : b \in B\}$ is an antichain, and so necessarily B is countable since \mathbb{Q} is ccc.. \square

\square

Lemma 5.11. *If \mathbb{Q} is ccc, then \mathbb{Q} preserves cardinals.*

Proof. First notice that regardless of \mathbb{Q} , if $\kappa \in M[G]$ is a cardinal then it is also a cardinal in M . For if κ failed to be a cardinal in M , there would be some ordinal $\alpha < \kappa$ and a bijection $f : \alpha \rightarrow \kappa$ with $f \in M$. But then f would also belong to $M[G]$ and in fact κ would not have been a cardinal in $M[G]$ after all.

So we just have to show that if $\kappa \in M$ and $M \models$ “ κ is a cardinal” and $M[G] \models$ “ κ is a cardinal” as well. Suppose for contradiction that κ is not a cardinal in $M[G]$. Then there is an ordinal $\alpha < \kappa$ and a function $f : \alpha \rightarrow \kappa$ which is surjective. Apply Lemma 5.10 to get a function $F \in M$ with $F : \alpha \rightarrow \mathcal{P}(\kappa)$, $f(\beta) \in F(\beta)$ for each $\beta < \alpha$, and for each $\beta < \alpha$ $F(\beta)$ is countable (within M).

Notice that $\kappa = \bigcup_{\beta < \alpha} F(\beta)$. This is because f was surjective; so if $\gamma \in \kappa$ there is some β such that $f(\beta) = \gamma$; then $f(\beta) \in F(\beta)$. This union is definable in M , since $F \in M$ and so $M \models |\kappa| \leq |\alpha| \cdot |\omega|$. That is $M \models |\kappa| \leq |\alpha|$. But that is a contradiction, since $\alpha < \kappa$ and κ is supposedly a cardinal in M . \square

Thus ω_2 is the same in M and $M[G]$, and hence $M[G] \models \omega_2 \leq 2^\omega$. So we have proved the following.

Theorem 5.12. *Let M be a countable transitive model of ZFC. There is a poset $\mathbb{P} \in M$ so that for any \mathbb{P} -generic G over M we have that $M[G] \models \neg CH$.*

We have now almost proved the independence of the continuum hypothesis. We must make a metamathematical argument to finish things off. For the following, ψ will stand for either CH or $\neg CH$. We have shown that if M is a countable transitive model of ZFC that there is a poset \mathbb{P} in M such that a given \mathbb{P} -generic filter G yields a countable transitive $M[G]$ satisfying ZFC and ψ .

Now the problem is we have no reason to believe that there is a countable transitive model of ZFC (and indeed there need not be). But we can get around this. To show that ψ is consistent with ZFC it is enough to show that $ZFC \not\vdash \neg\psi$. Now, if $ZFC \vdash \neg\psi$ there would be a proof of $\neg\psi$ from finitely many of the axioms of ZFC; that is there would be a finite fragment of ZFC say ϕ (remember by a finite fragment of ZFC we mean a conjunction of finitely many of the axioms of ZFC) so that $\phi \vdash \neg\psi$. So in order to prove that $ZFC \not\vdash \neg\psi$ it is in fact enough to show that every finite fragment of ZFC is consistent with ψ . So let ϕ be a fixed such fragment.

Now here is the crucial point. In proving that $M[G]$ satisfied ψ we only actually used finitely many of the axioms in ZFC; that is examining our earlier proofs one can see that there is a finite fragment χ of ZFC such that if $M \models \chi$ then $M[G] \models \psi$. Further, when we showed that $M[G]$ satisfied ZFC, for each axiom we only used finitely many of the axioms in M to get $M[G]$ to satisfy that axiom. So there is a finite fragment σ of ZFC such that if $M \models \sigma$ then $M[G] \models \phi$.

Now by Theorem 3.31 there is a countable transitive M such that $M \models \sigma \wedge \chi$. Then $M[G] \models \phi \wedge \psi$. Thus ϕ is consistent with ψ , as desired.

Thus we have proved that the continuum hypothesis is independent of the other axioms of set theory.

5.3 The Exact Value of the Continuum

When $\mathbb{P} = \text{Fn}(\omega \times \kappa, 2)$ and G is a \mathbb{P} -generic filter, then $M[G]$ is usually referred to as the *Cohen model* (for κ). We have shown that in the Cohen model we have that $2^\omega \geq \kappa$, but that doesn't tell us what the precise value is. In this section we'll explore the techniques that allow us to determine the exact value. The trick is to come up with a canonical set of names representing subsets of ω in the generic extension, and then count the names.

Definition 5.13. *A nice name for a subset of ω is a name $\tau \in M^{\mathbb{P}}$ of the form $\bigcup \{ \check{n} \times A_n : \pi \in \text{dom}(\sigma) \}$, where each A_n is an antichain of \mathbb{P} .*

Lemma 5.14. *Let $X \subseteq \omega$ be an element of $M[G]$. Then there is a nice name τ such that $\tau[G] = X$.*

Proof. Since $X \in M[G]$ there some $\sigma \in M^{\mathbb{P}}$ such that $\sigma[G] = X$. Now it need not be the case that σ is a nice name, but we will find a nice name τ with $\tau[G] = \sigma[G]$.

Working in M , let $n \in \omega$ be given. Using Zorn's lemma, take A_n to be a maximal antichain of conditions p so that $p \Vdash n \in \sigma$. Then we let τ be the corresponding nice name $\tau = \bigcup \{ \{ \check{n} \} \times A_n : \pi \in \text{dom}(\sigma) \}$. We claim that $\sigma[G] = \tau[G]$.

It is not hard to see that $\tau[G] \subseteq \sigma[G]$. For suppose $x \in \tau[G]$. Then there is some π and some $p \in G$ so that $x = \pi[G]$ and $\langle \pi, p \rangle \in \tau$. By definition of τ , $\pi = \check{n}$ for some n where $p \in A_n$. So $x = n$. By definition of A_n , $p \Vdash n \in \sigma$. Since $p \in G$, by definition of \Vdash we have $n \in \sigma[G]$.

Let us show that $\sigma[G] \subseteq \tau[G]$. Suppose $x \in \sigma[G]$; then $x = n$ for some $n \in \omega$. It is enough for us to show that there is some $p \in G \cap A_n$; if we had that then $\langle \check{n}, p \rangle \in \tau$ and $p \in G$ we should have $n \in \tau[G]$.

Suppose to the contrary that $A_n \cap G$ is empty. We claim that there is a $q \in G$ which is incompatible with every member of A_n . To see this, let

$$D = \{ q \in \mathbb{P} : q \text{ is below some member of } A_n \text{ or } q \text{ is incompatible with every member of } A \}$$

. Then $D \in M$ since D is defined using elements of M . We claim that D is dense. For suppose $p \in \mathbb{P}$ is arbitrary. If p is compatible with some $r \in A_n$ then if we take $q \leq p, r$ then $q \in D$. And if p is not compatible with some $r \in A_n$ then by definition $p \in D$ already.

Since G is \mathbb{P} -generic we can get $q \in D \cap G$. Since $G \cap A_n$ is empty we cannot have that q is below some member of A_n , for filters are closed upwards. Thus q is incompatible with every member of A_n .

Now let $s \in G$ with $s \Vdash n \in \sigma$. Let $r \leq q, s$. Then r is incompatible with every member of A_n as well, since $r \leq q$. Also $r \Vdash n \in \sigma$. But then $A_n \cup \{r\}$ is a larger antichain than A_n with every condition $a \in A_n$ giving $a \Vdash n \in \sigma$. This contradicts our choice of A_n . \square

Now we can do our counting.

Theorem 5.15. *Suppose M is a countable transitive model of set theory, and in M we take $\mathbb{P} = \text{Fn}(\omega \times \kappa, 2)$, where κ is some cardinal. Suppose that, in M , $\kappa^\omega = \kappa$. Then in $M[G]$, $2^\omega = \kappa$.*

Proof. We have already seen that in $M[G]$ we have $2^\omega \geq \kappa$. Let us show that $2^\omega \leq \kappa$.

First we count the number of nice names for subsets of ω . Let N equal

$$\{ \tau : \tau \text{ is a nice name for a subset of } \omega \}$$

. Since $|\mathbb{P}| = \kappa$ and \mathbb{P} is ccc, there are $(\kappa^\omega)^M = \kappa$ many antichains of \mathbb{P} in M . A nice name can clearly be viewed as a function mapping an element of ω to an antichain, and so there are $(\kappa^\omega)^M = \kappa$ many nice names. That is, $|N| = \kappa$.

But, in $M[G]$ there is a surjection from S to $\mathcal{P}(\omega)$, namely the map which sends τ to $\tau[G]$. Thus $2^\omega \leq \kappa$. \square

If, for example, the GCH holds in the ground model then for κ with cofinality greater than ω , we always have $\kappa^\omega = \kappa$. If we take for granted Gödel's result that the GCH is consistent then it follows that we can make the continuum take any value we like of uncountable cofinality.