SET THEORETICAL FORCING

Spring 2016

Tapani Hyttinen

Forcing is a method of proving that some claim ϕ is not provable from ZFC i.e. from the standard axiomatization of set theory (assuming the consistency of ZFC). If one also proves that $\neg\phi$ is not provable from ZFC i.e. ϕ is independent of ZFC, then one has shown that the truth of the claim ϕ can not be decided using generally accepted principles of mathematics as they stand today.

In these lectures we will be more interested in how to use forcing than all the details of the proofs of the validity of the method. We will follow the approach of K. Kunen's excellent book [Ku], which is also the recommended reference for anyone wanting to learn more.

Contents

1. Preliminaries

When one studies forcing it is necessary to take a formal approach to set theory. So our set theory ZFC is a first-order theory in a vocabulary $\{\in\}$, where $\in$ is a binary predicate symbol. However, for an obvious reason, we often avoid using first-order expressions (there are cases in which first-order formulas give the most convenient way of expressing claims) and instead use English (or something that looks a bit like English) and assume that, if needed, everyone can translate the sentences to the formal first-order language. Also we assume that we have a universe of (all) sets called V, that is a model of ZFC and we work inside V (until we construct a generic extension). In this first section, this assumption can be seen just as a normal practice of precenting proofs in mathematics. However later we really need V and this is a potential problem, since ZFC (and thus current mathematics) can not prove the existence of V (by Gödel's second incompleteness theorem). Later for partially ordered sets P, we will also assume the existence of so called P-generic filter G over V. In general ZFC can not prove the existence of G either. In Section 5 we will look at the question, why these assumptions are not a problem.

Elements of V are called sets and subsets of V, which are first-order definable with parameters, are called classes. If $\phi(v_0, ..., v_n)$ is a first-order $\{\in\}$-formula and $a_1, .., a_n$ are sets, then the expression $\phi(v_0, a_1, ..., a_n)$ is called a property and for a set x, we write $\phi(x, a_1, ..., a_n)$ (in this section, from Section 2 on, we need to be more specific) if, using the notation from Matemaattinen Logiikka course,

$$V \models_{s(x/0)(a_1/1),...,(a_n/n)} \phi$$

and say that x has the property $\phi(v_0, a_1, ..., a_n)$. Often we do not mention the parameters and just say that x has the property ϕ and write just $\phi(x)$. So the classes are families of sets that have some fixed property ϕ.

1.1 Axioms

We sart by giving the axioms of ZFC.

I Extensionality: If sets a and b have the same elements, then $a = b$.

Notice, that also the inverse of the implication in Extensionality holds. And that from now on to determine a set, it is enough to describe its elements, e.g. $\{3, 8, i\}$, $\{n \in \mathbb{N} | \; n \text{ is even}\}$,..., and of course $\emptyset$. Also we extend the idea in Extensionality to classes i.e. two classes are considered the same if they have the same elements and a class and a set are considered the same if they have the same elements.

1.1.1 Exercise. *Show that every set is a class.*

II Foundation: Every non-empty set a has an $\in$-minimal element i.e. there is $x \in a$ such that for all $y \in a$, $y \notin x$.

III Pairing: For any sets a and b, $\{a,b\}$ is a set.

Notice, that from Pairing it follows that for every set a, $\{a\}$ is a set.

1.1.2 Exercise. *Show that there is no set a such that $a \in a$ or sets a and b such that $a \in b \in a$.*

IV Separation (aka Comprehension): If a is a set and ϕ is a property, then $\{x \in a|\ \phi(x)\}$ is a set.

V Union: For every set a, the union $\cup a$ of the elements of a is a set ($x \in \cup a$ if $x \in b$ for some $b \in a$).

1.1.3 Exercise.
(i) Show that if a, b, c, d and e are sets, then $\{a, b, c, d, e\}$ is a set.
(ii) We write (a, b) for the set $\{a, \{a, b\}\}$. Show that
(a) (a, b) is indeed a set,
(b) if $(a, b) = (c, d)$, then $a = c$ and $b = d$.

VI Power Set: For every set a, the power set $P(a)$ of a is a set ($x \in P(a)$ if $x \subseteq a$ i.e. for every set y, if $y \in x$, then $y \in a$).

So far we have had no axiom that states that there exists even a single set. The next axiom says that there is an infinite set. However, it seems to assume that the empty set already exists. So should we not have an axiom that says this? There is no need for this: Even without any assumptions, in first-order logic one can always prove that there exists x such that $x = x$. So in the case of set theory, one can always prove the existence of at least one set.

1.1.4 Exercise.
(i) Show that the empty set $\emptyset$ exists.
(ii) For sets a and b, show that $a \times b = \{(x, y)|\ x \in a,\ y \in b\}$ is a set.

VII Infinity: There exists an inductive set i.e. a set a such that $\emptyset \in a$ and if $x \in a$, then also $x \cup \{x\} \in a$ (exercise: show that $x \cup \{x\}$ is a set).

When we talk about functions f from a set a to a set b, we always mean that $f = \{(x, f(x))|\ x \in a\}$ is a set. We talk also about class functions:

1.1.5 Definition. *Let C be a class. We say that a function $F : C \to V$ is a class function if the graph of F is a class i.e. there is a property ϕ such that for all sets x, x has the property ϕ iff $x = (a, F(a))$ for some set $a \in C$.*

VIII Replacement: If a is a set and $F : a \to V$ is a class function, then $\{F(x) | \; x \in a\}$ is a set.

1.1.6 Exercise.

(i) Show that if a is a set and $F : a \to V$ is a class function, then F is a set.

(ii) Show that if a and b are sets and $f : a \to b$ is a function, then it is a class function.

IX Choice: If a is a set and every $x \in a$ is non-empty, then there is a function $f : a \to \cup a$ such that for all $x \in a$, $f(x) \in x$.

The theory that consists of all these axioms is called ZFC. If the Choice is left out, the resulting theory is called just ZF. Unless we state otherwise, we work in ZFC.

1.2 Recursive definitions

1.2.1 Definition.

(i) If C is a class, then a class $<$ is called a partial ordering of C if the elements of $<$ are of the form (x,y), $x,y \in C$, and the following holds: if $(x,y),(y,z) \in <$, then $(x,z) \in <$ and $(y,x) \notin <$. Instead of writing $(x,y) \in <$, we will simply write $x < y$.

(ii) A partial ordering $<$ is a linear ordering, if in addition, for all $x,y \in C$, $x < y$ or $x = y$ or $y < x$.

(iii) A partial ordering is well-founded if for all $x \in C$, $\{y \in C | \; y < x\}$ is a set and if a is a non-empty set such that every element of it belongs to C, then a has a $<$-minimal element. If in addition the partial ordering is a linear ordering, it is called a well-ordering.

If $<$ is a partial ordering of C, then by $\leq$ we mean the relation $a \leq b$ if $a < b$ or $a = b$.

1.2.2 Theorem. *Suppose C is a class and $<$ is a well-founded partial ordering of C. Let ϕ be a property and assume that for all $x \in C$, if every element of $\{y \in C | \; y < x\}$ has the property ϕ, then also x has it. Then every element of C has the property ϕ.*

Proof. Suppose not. Let $x \in C$ be such. We show first that we can choose x so that it is $<$-minimal element of C among those that do not have the property ϕ: If x is not such then the class a of all element of C which are smaller than x and do not have the property ϕ is non-empty and a set. Since $<$ is well founded, a has a $<$-minimal element. Clearly this is as wanted.

But if x is a minimal among those that do not have the property ϕ, then every element of $\{y \in C | \; y < x\}$ has the property, and so also x has it, a contradiction. □

1.2.3 Theorem. *Suppose C is a class, $<$ is a well-founded partial ordering of C and $G : V \to V$ is a class function. Then there is a unique class function $F : C \to V$ such that for all $x \in C$, $F(x) = G(F \restriction C_x)$, where $C_x = \{y \in C|\ y < x\}$.*

Proof. We say that $A \subseteq C$ is downward closed if $x < y \in A$ implies $x \in A$. We start with an exercise:

1.2.3.1 Exercise. *Suppose that a set $A \subseteq C$ is downward closed and $f, g : A \to V$ (recall Exercise 1.1.6) are such that for all $z \in A$, $f(z) = G(f \restriction C_z)$ and $g(z) = G(g \restriction C_z)$ (notice that $C_z \subseteq A$). Show that $f = g$. Conclude that if F exists, it is unique.*

Now let ϕ the following property of sets a: a is of the form (x, y) where $x \in C$ and y is such that there is a function $f_x : C_x \to V$ such that $y = G(f_x)$ and for all $z \in C_x$, $f(z) = G(f_x \restriction C_z)$. We will show that for every $x \in C$, there is a set y such that (x, y) has the property ϕ. Then since by Exercise 1.2.3.1, such y is unique, ϕ defines a class function $C \to V$.

To see that y exists, it is enough to show that f_x exists. We prove this by induction i.e. by using Theorem 1.2.2. So suppose that the claim holds for every $z \in C_x$. We notice

(*) if $z, w \in C$ and f_z and f_w exist, then $f_z \restriction (C_z \cap C_w)$ and $f_w \restriction (C_z \cap C_w)$ satisfy the requirements of Exercise 1.2.3.1 for $A = (C_z \cap C_w)$ and thus $f_z \restriction (C_z \cap C_w) = f_w \restriction (C_z \cap C_w)$.

So by (*), if C_x does not have maximal elements ($z \in C_x$ is maximal if there are no $y \in C_x$ such that $z < y$) $f_x = \bigcup_{z<x} f_z$ is as wanted. (Notice that we use replacement axiom here.) On the other hand, if C_x has maximal elements, we simply let $f_x = (\bigcup_{z<x} f_z) \cup \{(z, G(f_z))|\ z \in C_x \textit{ is maximal}\}$. Again by (*), f_x is as wanted.

So we are left to prove that for all x, $F(x) = G(F \restriction C_x)$. So suppose that this holds for all $z \in C_x$ and let f_x be as in the definition of ϕ. Then by Exercise 1.2.3.1, $F \restriction C_x = f_x$ and thus $F(x) = G(f_x) = G(F \restriction C_x)$. □

1.3 Ordinals

1.3.1 Definition.

(i) We say that a set a is transitive if $x \in y \in a$ implies $x \in a$ (i.e. $\cup a \subseteq a$ and notice that if a and b are transitive, then so is $a \cap b$).

(ii) We say that a set α is an ordinal if it is transitive and linearly ordered by $\in$. For ordinals α and β, one usually writes $\alpha < \beta$ instead of $\alpha \in \beta$ and $\alpha \le \beta$ for $\alpha < \beta$ or $\alpha = \beta$.

(iii) The class of all ordinals is denoted by On.

1.3.2 Exercise.

(i) Show that ordinals are well-ordered by $\in$.

(ii) Show that $0 = \emptyset$ is an ordinal.

(iii) Show that if α is an ordinal, then also $\alpha + 1 = \alpha \cup \{\alpha\}$ is an ordinal.

(iv) Show that if a is a set of ordinals and for all $\alpha, \beta \in a$, either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$, then $\cup a$ is an ordinal.

(v) Show that if α is an ordinal and $\beta \in \alpha$, then β is an ordinal.

(vi) Show that if α and β are ordinals, then so is $\alpha \cap \beta$.

1.3.3 Lemma. *Let α and β be ordinals.*

(i) If $\alpha \subseteq \beta$, then either $\alpha = \beta$ or $\alpha \in \beta$.

(ii) Either $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$.

Proof. (i): Suppose $\alpha \neq \beta$. Then $\beta - \alpha$ is not empty and thus it has the least element γ. If $\delta \in \gamma$, then $\delta \in \beta$ and so by the choice of γ, $\delta \in \alpha$. On the other hand, if $\delta \in \alpha$, then $\gamma \not\leq \delta$, because otherwise $\gamma \in \alpha$ and this is against our choice of γ. Thus since $\in$ linearly orders β, $\delta \in \gamma$. It follows that $\alpha = \gamma$ and so $\alpha \in \beta$.

(ii): Now by Exercise 1.3.2 (vi), $\gamma = \alpha \cap \beta$ is an ordinal. Then $\gamma = \alpha$ or $\gamma = \beta$ because otherwise by (i), $\gamma \in \alpha \cap \beta = \gamma$. In the first case $\alpha \subseteq \beta$ and in the other case $\beta \subseteq \alpha$. □

1.3.4 Exercise.

(i) Show that On is well-ordered by $\in$.

(ii) Show that $\alpha + 1$ is the least ordinal strictly greater than the ordinal α.

(iii) For a set a of ordinals show that $\cup a$ is the supremum of a (in particular, $\cup a$ is an ordinal).

1.3.5 Definition.

(i) We say that an ordinal α is a successor ordinal if $\alpha = \beta + 1$ for some ordinal β and otherwise α is called a limit ordinal. However, 0 is usually not considered a limit ordinal.

(ii) By ω we denote the least limit ordinal $\neq 0$ (if such ordinal exists).

1.3.6 Lemma. *For every ordinal β there is a limit ordinal $\alpha > \beta$.*

Proof. We show first that ω exists. By Infinity, there is an inductive set b. Let $a = b \cap On$ and $\alpha = \cup a$. By Exercise 1.3.4 (iii), α is an ordinal. Also it is easy to see that a is inductive and thus α can not be a successor ordinal. So in particular ω exists.

Now for given ordinal β, choose a function $f : \omega \to On$ so that $f(0) = \beta$ and for successor ordinals $\gamma + 1 \in \omega$, $f(\gamma + 1) = f(\gamma) + 1$ (exercise: show that f exists and $rng(f) \subseteq On$, keep in mind that every ordinal in ω excluding 0, is a successor ordinal). Let $\alpha = \cup rng(f)$. Clearly α is as wanted. □

1.3.7 Exercise. *Show that there is no class function $f : \omega \to V$ such that for all $n \in \omega$, $f(n + 1) \in f(n)$.*

1.3.8 Theorem. *For every set a there is an ordinal α and a one-to-one and onto function $f : \alpha \to a$.*

Proof. Let b be the set of all non-empty subsets of a and g be the choice function for b. We define a class function $G : V \to V$ so that for all ordinals β and functions $h : \beta \to a$ with $rng(h) \neq a$, $G(h) = g(a - rng(h))$ and for all other sets x, $G(x) = a$. Let $F : On \to V$ be such that for all ordinals γ, $F(\gamma) = G(F \restriction \gamma)$ (by Theorem 1.2.3) and suppose that for some ordinal γ, $F(\gamma) = a$. Then by letting α be the least such ordinal, α and $f = F \restriction \alpha$ are clearly as wanted.

So it is enough to show that for some γ, $F(\gamma) = a$. Suppose not. Then (by Separation) F^{-1} is a class function from a subset of a onto On. Thus by Replacement On is a set. Thus $\beta = \cup On$ is an ordinal. So $\beta \in \beta + 1 \in On$ and thus $\beta \in \beta$, a contradiction. □

1.3.9 Exercise. *(Zermelo's well-ordering theorem) Every set can be well-ordered.*

In fact, under e.g. ZF, Zermelo's well-ordering theorem is equivalent with Choice: To get Choice, simply choose a well-ordering $<$ for $\cup a$ and then for every $x \in a$, let $f(x)$ be the $<$-least element of x.

The sets V_α in the next exercise form so called cumulative hierarchy.

1.3.10 Exercise. *We define V_α for all ordinals α as follows: $V_0 = \emptyset$, $V_{\alpha+1} = P(V_\alpha)$, and for limit ordinals α, $V_\alpha = \cup_{\gamma<\alpha} V_\gamma$. Show that*
(i) $\alpha \mapsto V_\alpha$ is a class functions,
(ii) for $\gamma < \alpha$, $V_\gamma \subseteq V_\alpha$,
(iii) for all sets a there is an ordinal α such that $a \in V_\alpha$.

1.3.11 Exercise. *For all x let $TC(x)$ be the class of those y for which there are $0 < n < \omega$ and x_i, $i \leq n$, such that $x_0 = y$, $x_n = x$ and for all $i < n$, $x_i \in x_{i+1}$ (i.e. $TC(x)$ is the least transitive set a such that $x \subseteq a$). Show that for all x, $TC(x)$ is a set.*

1.4 Cardinals

1.4.1 Definition. *We say that sets a and b have the same cardinality, if there is a one-to-one and onto function $f : a \to b$.*

1.4.2 Exercise.
(i) Show that the equicardinality relation from Definition 1.4.1 is an equivalence relation.
(ii) Show that if there is an onto function $f : a \to b$, then there is a one-to-one function $g : b \to a$ and vice versa assuming that $b \neq \emptyset$.

1.4.3 Theorem. *(Cantor-Bernstein) For all sets a and b, if there are one-to-one functions $f : a \to b$ and $g : b \to a$, then a and b have the same cardinality.*

Proof. For all $n \in \omega$, we define sets A_n and B_n as follows: $A_0 = a$, $B_0 = b$, $A_{n+1} = g(f(A_n))$ and $B_{n+1} = f(g(B_n))$. Finally, let $A = \bigcap_{n<\omega} A_n$ and $B = \bigcap_{n<\omega} B_n$. Clearly, for $n < \omega$, $A_{n+1} \subseteq A_n$ and $B_{n+1} \subseteq B_n$. Also (e.g. draw a picture) $f \restriction (A_n - g(B_n))$ is one-to-one function from $A_n - g(B_n)$ onto $f(A_n) - B_{n+1}$,

$g^{-1} \restriction (g(B_n) - A_{n+1})$ is one-to-one function from $g(B_n) - A_{n+1}$ onto $B_n - f(A_n)$ and $f \restriction A$ is one-to-one function from A onto B. By putting these together, the required one-to-one and onto function is found. □

1.4.4 Definition.

(i) We say that an ordinal α is a cardinal if there are no $\beta < \alpha$ and a one-to-one function from α to β.

(ii) We say that a set a is finite, if for all one-to-one functions $f : a \to a$, $rng(f) = a$.

1.4.5 Lemma. *ω and every $n \in \omega$ are cardinals. In fact, every $n \in \omega$ is finite.*

Proof. We start by proving the claim for the elements of ω. Clearly it is enough to show that they are finite. We prove this by induction (i.e. using Theorem 1.2.2, keeping in mind that all elements of ω, excluding 0, are successor ordinals and, in fact, the claim we prove is that every ordinal α is either finite or $\geq \omega$).

For $n = 0$, this is clear. So suppose that this holds for n and let $f : n+1 \to n+1$ be one-to-one. For a contradiction suppose that $rng(f) \neq n + 1$. By applying a transposition, we may assume that $n \notin rng(f)$. But then $f \restriction n$ is a one-to-one function from n to a proper subset of n, a contradiction.

If ω is not a cardinal, then there are $n \in \omega$ and a one-to-one function $f : \omega \to n$. But then $f \restriction n + 1$ contradicts what we just proved. □

1.4.6 Exercise.

(i) Show that an ordinal α is finite iff $\alpha \in \omega$.

(ii) Show that all infinite cardinals are limit ordinals.

(iii) Show that if a is a set of cardinals, then $\cup a$ is a cardinal.

1.4.7 Lemma. *For every set a, there is a unique cardinal κ for which there is a one-to-one function from κ onto a.*

Proof. Clearly there cannot be more than one such cardinal. So we prove just the existence: Let κ be the least ordinal such that there is a one-to-one function f from κ onto a (such κ exists by Theorem 1.3.8). It is enough to show that κ is a cardinal. If not, then there is $\alpha < \kappa$ and a one-to-one function $g : \kappa \to \alpha$. By Cantor-Bernstein, we can choose g so that it is also onto. But then α and $f \circ g^{-1}$ witness that κ was not minimal. □

1.4.8 Definition. *Let a be a set. The unique cardinal κ for which there is a one-to-one function from κ onto a, is called the cardinality of a and is denoted by $|a|$. If the cardinality of a set is $\leq \omega$, we say that the set is countable.*

1.4.9 Exercise.

(i) Show that a set a is finite iff $|a| \in \omega$.

(ii) Show that $|a| \leq |b|$ iff there is a one-to-one function $f : a \to b$.

(iii) Show that if a and b are finite, then so is $a \cup b$.

The elements of ω are called natural numbers and thus ω is called also the set of natural numbers i.e. $\mathbb{N}$. We also write $0 = \emptyset$ as already mentioned and $1 = 0 + 1 = 0 \cup \{0\}$, $2 = 1 + 1$, $3 = 2 + 1$ etc. Recall that for all $n \in \omega$, $n = \{0, 1, ..., n - 1\}$.

1.4.10 Theorem. *For all non-empty sets* a *and* b, *if one of them is infinite, then* $|a \times b| = max\{|a|, |b|\}$.

Proof. Clearly, it is enough to prove that for all infinite cardinals κ, $|\kappa \times \kappa| = \kappa$. For this it is enough to find a one-to-one function from $\kappa \times \kappa$ to κ. We order the elements of $On \times On$ so that $(\alpha, \beta) < (\gamma, \delta)$ if one of the following holds:
(i) $max\{\alpha, \beta\} < max\{\gamma, \delta\}$,
(ii) $\alpha < \gamma \leq max\{\alpha, \beta\} = max\{\gamma, \delta\}$,
(iii) $\alpha = max\{\alpha, \beta\} = max\{\gamma, \delta\} = \gamma$ and $\beta < \delta$.

1.4.10.1 Exercise. *Show that* $<$ *is a well-ordering of* $On \times On$.

Using Theorem 1.2.3, define $\Gamma : On \times On \to On$ so that for all $x \in On \times On$, $\Gamma(x)$ is the least ordinal (strictly) greater than every element in $rng(\Gamma \restriction (On \times On)_x)$ (for this notation, see Theorem 1.2.3).

1.4.10.2 Exercise. *Show that* F *is strictly increasing and that if* $\Gamma(\alpha, \beta) = \gamma$ *and* $\gamma' < \gamma$, *then there is* $(\alpha', \beta') < (\alpha, \beta)$ *such that* $\Gamma(\alpha', \beta') = \gamma'$.

By Exercise 1.4.10.2, it is enough to show that for infinite cardinals κ, $rng(\Gamma \restriction (\kappa \times \kappa)) \subseteq \kappa$. We do this by induction. The case when $\kappa = \omega$ is left as an exercise. So suppose $\kappa > \omega$. For a contradiction suppose that there are $\alpha, \beta < \kappa$ such that $\Gamma(\alpha, \beta) \geq \kappa$. Let $\lambda = max\{|\alpha|, |\beta|\} < \kappa$. Then by Exercise 1.4.10.2, $\Gamma^{-1} \restriction \kappa : \kappa \to (On \times On)_{(\alpha,\beta)}$ is one-to-one and by the induction assumption (from which it follows that if $|a|, |b| \leq \lambda$, then $|a \times b| \leq \lambda$), $|(On \times On)_{(\alpha,\beta)}| \leq |max\{\alpha, \beta\} \times max\{\alpha, \beta\}| = |\lambda \times \lambda| = \lambda$, a contradiction. □

As a hint for the item (i) in next exercise we want to mention that the claim in the item can not be proved without Choice. If Choice is not assumed, it is possible that the set of reals is a countable union of countable sets and we will see later that the set of reals is not countable and this can be proved without Choice.

Also, instead of talking about functions $f : I \to X$ for some sets I and X, it is sometimes notationally convenient to talk about indexed sequences $(x_i)_{i \in I}$. So by an indexed sequence $(x_i)_{i \in I}$ we simply mean a function $f : I \to V$ such that for all $i \in I$, $f(i) = x_i$. Thus for $x : a \to V$, we sometimes also write x_i in place of $x(i)$.

1.4.11 Exercise.

(i) Suppose κ *is an infinite cardinal and* a *is a set of cardinality* $\leq \kappa$ *such that also every element of it is of cardinality* $\leq \kappa$. *Show that* $|\cup a| \leq \kappa$. *In particular, for all sets* a *and* b, *if one of them is infinite, then* $|a \cup b| = max\{|a|, |b|\}$.

(ii) For all infinite cardinals κ, *show that there are sets* $X_i \subseteq \kappa$, $i \in \kappa$, *such that for all* i, *the cardinality of* X_i *is* κ *and for all* $i \neq j$, $X_i \cap X_j = \emptyset$.

(iii) Show that the set of rational numbers is countable.

For sets a and b, by a^b we mean the set of all functions from b to a (e.g. $\mathbb{N}^n$). If $b=\beta$ is an ordinal we also write $a^{<\beta}$ for $\bigcup_{\alpha<\beta} a^\alpha$ and $a^{\le\beta}$ for $\bigcup_{\alpha\le\beta} a^\alpha$. On the level of notation, we also identify $f:2\to X$ with $(f(0),f(1))$ and thus think that $X\times X$ is the same as X^2, see the discussion on indexed sequences above.

1.4.12 Lemma. *For all cardinals κ, $|P(\kappa)|=|2^\kappa|$ and if κ is infinite, then $|2^\kappa|=|(2^\kappa)^\kappa|=|2^{(\kappa\times\kappa)}|=|\kappa^\kappa|$.*

Proof. For $|P(\kappa)|=|2^\kappa|$, just map every $a\subseteq\omega$ to its characteristic function. $|2^\kappa|=|2^{\kappa\times\kappa}|$ is clear by Lemma 1.4.10. To find a one-to-one function F from $2^{\kappa\times\kappa}$ onto $(2^\kappa)^\kappa$, simply for $\eta\in 2^{\kappa\times\kappa}$ let $\xi=F(\eta)$ be such that for all $n,m<\kappa$, $(\xi(n))(m)=\eta(n,m)$. Since $2^\kappa\subseteq\kappa^\kappa$, $|2^\kappa|\le|\kappa^\kappa|$. Finally since $\kappa\le|2^\kappa|$, it is easy to see that $|\kappa^\kappa|\le|(2^\kappa)^\kappa|$. □

One often denotes $|2^\kappa|$ by just 2^κ. It is clear from the context which possibility we mean.

1.4.13 Theorem. *For all sets a, $|P(a)|>|a|$.*

Proof. Clearly it is enough to prove the claim in the cases when a is some cardinal κ, i.e. that $2^\kappa>\kappa$. For finite cardinals the claim is clear and so suppose κ is infinite. For a contradiction, suppose $2^\kappa\le\kappa$. Clearly, $2^\kappa\ge\kappa$ and thus, under the counter assumption, there is a one-to-one function f from κ onto 2^κ. Denote $f(\alpha)$ by ξ_α.

Let $g:\kappa\to 2$ be such that for all $\alpha<\kappa$, $g(\alpha)=1-\xi_\alpha(\alpha)$. Then $g\in 2^\kappa$ and so for some $\alpha<\kappa$, $g=\xi_\gamma$. Now $g(\gamma)=1-\xi_\gamma(\gamma)=1-g(\gamma)$, a contradiction. □

1.4.14 Definition. *Let γ be a limit ordinal.*

(i) The cofinality $cf(\gamma)$ of γ is the least ordinal α such that there is a function $f:\alpha\to\gamma$ such that $\cup rng(f)=\gamma$.

(ii) γ is called regular if $cf(\gamma)=\gamma$.

1.4.15 Exercise.

(i) Show that for all limit ordinals γ, $cf(\gamma)$ is a regular cardinal. Conclude that regular ordinals are cardinals.

(ii) Show that ω is a regular cardinal.

1.4.16 Definition. *If κ is a cardinal, then the least cardinal λ greater that κ is denoted by κ^+. If κ is λ^+ for some cardinal λ, it is called a successor cardinal and otherwise it is a limit cardinal.*

1.4.17 Exercise.

(i) Show that for all ordinals α, there is a cardinal $\kappa>\alpha$.

(ii) Show that every infinite successor cardinal is regular.

(iii) Let X, Y, I and α_i and f_i, $i\in I$, be as in Definition 1.5.1 (ii). Suppose further that κ is a regular cardinal such that for all $i\in I$, $\alpha_i<\kappa$. Then $C(Y,f_i)_{i\in I}=C_\kappa(Y,f_i)_{i\in I}$.

We finish this section by defining a class function $\alpha\mapsto\omega_\alpha$ (sometimes ω_α is also denoted by $\aleph_\alpha$).

1.4.18 Definition. *We define* ω_α *for all ordinals* α *as follows:* $\omega_0 = \omega$, $\omega_{\alpha+1} = \omega_\alpha^+$ *and for limit ordinals* α, $\omega_\alpha = \cup_{\gamma<\alpha}\omega_\gamma$.

1.5 Recursive definitions revisited

1.5.1 Definition. *Suppose* X *is a set.*

(i) Suppose α *is an ordinal,* $f : X^\alpha \to X$ *is a function and* $C \subseteq X$. *We say that* C *is closed under* f *if for all* $x \in C^\alpha$, $f(x) \in C$.

(ii) Suppose $Y \subseteq X$ *and for all* $i \in I$, α_i *is an ordinal and* $f_i : X^{\alpha_i} \to X$ *is a function. Then by* $C(Y, f_i)_{i\in I}$ *we mean the* $\subseteq$*-least subset* C *of* X *such that it contains* Y *and is closed under every* f_i, $i \in I$ *(if such* C *exists).*

1.5.2 Lemma. *Let* X, Y, I *and* α_i *and* f_i, $i \in I$, *be as in Definition 1.5.1 (ii). Then* $C(Y, f_i)_{i\in I}$ *exists.*

Proof. Just let $C(Y, f_i)_{i\in I}$ be the intersection of all sets $C \subseteq X$ which contain Y and are closed under every f_i (notice that X is such a set). □

1.5.3 Lemma. *Let* X, Y, I *and* α_i *and* f_i, $i \in I$, *be as in Definition 1.5.1 (ii). Suppose that* ϕ *is a property, every element of* Y *has it and for all* $k \in I$ *and* $x \in C(Y, f_i)_{i\in I}^{\alpha_k}$ *the following holds: If every* x_j, $j < \alpha_k$, *has the property, then also* $f_k(x)$ *has the property. Then every element of* $C(Y, f_i)_{i\in I}$ *has the property* ϕ.

Proof. Let C be the set of all elements of $C(Y, f_i)_{i\in I}$ that have the property ϕ. Then C contains Y and is closed under every f_i. Thus $C(Y, f_i)_{i\in I} \subseteq C$. □

1.5.4 Definition. *Let* X, Y, I *and* α_i *and* f_i, $i \in I$, *be as in Definition 1.5.1 (ii). For all ordinals* α, *we define* $C_\alpha(Y, f_i)_{i\in I}$ *as follows:*

(i) $C_0(Y, f_i)_{i\in I} = Y$,

(ii) $C_{\alpha+1}(Y, f_i)_{i\in I} = C_\alpha(Y, f_i)_{i\in I} \cup \{f_i(x)|\ i \in I,\ x \in (C_\alpha(Y, f_i)_{i\in I})^{\alpha_i}\}$,

(iii) if α *is limit, then* $C_\alpha(Y, f_i)_{i\in I} = \bigcup_{\beta<\alpha} C_\beta(Y, f_i)_{i\in I}$.

1.5.5 Exercise. *Show that* $\alpha \mapsto C_\alpha(Y, f_i)_{i\in I}$ *is a class function from On to* $P(X)$ *and that for all ordinals* $\alpha < \beta$, $Y \subseteq C_\alpha(Y, f_i)_{i\in I} \subseteq C_\beta(Y, f_i)_{i\in I} \subseteq C(Y, f_i)_{i\in I}$.

1.5.6 Lemma. *Let* X, Y, I *and* α_i *and* f_i, $i \in I$, *be as in Definition 1.5.1 (ii) and* κ *be a regular cardinal. Suppose further that for all* $i \in I$, $\alpha_i < \kappa$. *Then* $C(Y, f_i)_{i\in I} = C_\kappa(Y, f_i)_{i\in I}$.

Proof. By Exercise 1.5.5, it is enough to show that $C_\kappa(Y, f_i)_{i\in I}$ is closed under every f_k, $k \in I$. For this let $x \in (C_\kappa(Y, f_i)_{i\in I})^{\alpha_k}$. Since κ is regular, there is $\gamma < \kappa$ such that $x \in (C_\gamma(Y, f_i)_{i\in I})^{\alpha_k}$ (Exercise, think of function $g : \alpha_k \to \omega_1$ such that for all $\beta < \alpha_k$, $g(\beta)$ is the least ordinal δ for which $x_\beta \in C_\delta(Y, f_i)_{i\in I}$). But then $f_i(x) \in C_{\gamma+1}(Y, f_i)_{i\in I} \subseteq C_\kappa(Y, f_i)_{i\in I}$. □

2. Generic extension

The strategy to show that some first-order sentence ϕ is not provable from ZFC is to first find a suitable partial-order $P = (P, <)$ (i.e. a set P together with a partial-ordering $<$ of it) and a P-generic filter G over V and then construct a generic extension $V[G]$ and finally show that $V[G]$ is a model of ZFC together with $\neg\phi$. However, this construction can not be done inside V. It follows that we work outside V.

So the picture is as follows: We have two versions of ZFC. One is our meta theory ('the real ZFC') i.e. our foundations of mathematics, which can be though as a formal first-order theory but also as any other theory in mathematics in every day language (if a bit care is taken). For notational reasons, we think the meta theory also as a first-order theory. The other one is our object theory which is a coded version of the formal theory (we do not give the coding explicitly but assume that it is a natural one). The meta theory talks about the object theory as e.g. in the proof of Gödel's incompleteness theorem for PA in the course Matemaattinen logiikka; only now it is easier to think the formulas of the object theory as real formulas since in mathematics we are used to code mathematical object as sets much better than as natural numbers. In fact, we do not distinguish formulas from their codes. This is much what we do every time when we work with formal theories, only now we make this explicit. However, a bit care is needed here. On the object side existence means that our meta theory proves the existence and nothing else. Still we often follow the common practice in mathematics and talk about the object side as if we are working in a model of the meta theory.

To be able to talk about V in the meta theory, we think it as a constant and in meta theory assume that it satisfies the object ZFC i.e. that "$V \models \phi$" belongs to the meta theory for all axioms ϕ of (meta) ZFC. Of course, in set theory we can express everything that is needed about the object side e.g. to be a formula, to be an axiom of ZFC, to be true in a model, to be a proof etc. We simply write out the usual definitions in the meta theory. It is useful to notice that if on the meta side ZFC proves some sentence, then ZFC proves that the same is true on the object side. In particular, everything provable on the meta level is true in V.

In order to be able to do the constructions, we need to assume that the meta theory thinks that V is well-founded in the following sense (below when we talk about well-founded partial orderings of classes we mean in the sense of Definition 1.2.1): there are no $a_i \in V$, $i < \omega$, such that for all $i < \omega$, $a_{i+1} \in a_i$ in V. We also assume that the meta theory thinks that V is transitive in the following sense: Every element x of V is the set of all elements y that V thinks are elements of x. In particular, then every element of V is a subset of V. This simplifies our definitions.

2.1 Exercise. *Show that the transitivity assumption can be made without loss of generality.*

Finally, we are going to assume that V is countable. Recall that in Section 5, we will look at the questions: why all our additional assumptions are harmless and why finding $V[G]$ such that $V[G] \models \neg\phi$ shows that ZFC does not prove ϕ.

Let ϕ be a sentence (with possible parameters). Since we do not distinguish formulas and their codes and, as pointed out above, the truth in V is expressible in ZFC, we can talk about the truth of ϕ in V. We use ϕ^V as a shorthand for the sentence that says that ϕ is true in V. And so we can e.g. claim that $\phi^V \rightarrow \phi$. And we can do the same for formulas as well. E.g. claim $\forall v_0(v_0 \in V \rightarrow (\phi(v_0)^V \rightarrow \phi(v_0))$ makes sense. For a formula $\phi(v_0)$ with only v_0 free (but possibly with parameters from V), by ϕ^V we mean also the set of all $a \in V$ such that $V \models \phi(a)$. If ϕ^V contains just one element, we use ϕ^V also to denote that element e.g. ω^V is the element of V that satisfies the definition of ω.

Since we have assumed that V is transitive, for many sentences ϕ (with parameters from V), $\phi^V \leftrightarrow \phi$ is true (i.e. provable from in our meta theory) and when this is the case, we say that ϕ is absolute for V.

2.2 Exercise. *Let $a, b \in V$. Show that*
(i) $(a \in b)^V \leftrightarrow (a \in b)$.
(ii) (*"a is a partial order"*$)^V \leftrightarrow$ (*"a is a partial order"*).
(iii) $(a \in On)^V \leftrightarrow (a \in On)$.
(iv) $\omega^V = \omega$.
(v) $V_\omega^V = V_\omega$
(vi) $\forall x($*"x is a formula"* $\leftrightarrow (x \in V \wedge ($*"$x$ is a formula"*$)^V)$.

For this and the next section, we fix a partial order $P = (P, <) \in V$ with a largest element 1 (these are often called po-sets). For $a, b \in P$, we write $a || b$ if there is $c \in P$ such that $c \leq a, b$. If there is no such c, we write $a \perp b$.

2.3 Definition.

(i) We say that $D \in V$ is dense in P if $D \subseteq P$ and for all $a \in P$, there is $b \in D$ such that $b \leq a$.

(ii) We say that $G \subseteq P$ is a filter if the following holds:
(a) $1 \in G$,
(b) if $a \in G$ and $b \geq a$, then $b \in G$,
(c) if $a, b \in G$, then there is $c \in G$ such that $c \leq a, b$.

(iii) We say that G is P-generic over V if it is a filter and for all $D \in V$, if D is dense in P, then $G \cap D \neq \emptyset$.

2.4 Exercise.

(i) For all $D \in V$, (*"D is dense in P"*$)^V \leftrightarrow$ (*"D is dense in P"*).

(ii) Show that if G is P-generic over V and $p \in P$ is such that for all $q \in G$, $p || q$, then $p \in G$.

(iii) Suppose that for all $a \in P$, there are $b, c \in P$ such that $b, c < a$ and $b \perp c$. Show that if G is P-generic over V, then $G \notin V$.

(iv) Show that for all $p \in P$, there exists a P-generic G over V such that $p \in G$.

(v) Suppose G is P-generic over V, $p \in G$ and $C \subseteq P$ is such that that for all $q \leq p$ there is $r \leq q$ such that $r \in C$. Show that $C \cap G \neq \emptyset$.

2.5 Definition. *The set* V^P *of* P*-names is defined as follows:*

(i) $\emptyset$ *is a* P*-name.*

(ii) For all $\alpha \in On^V$, *and* $p_i \in P$, $i < \alpha$, *if for all* $i < \alpha$, τ_i *is a* P*-name and* $\tau = \{(\tau_i, p_i) | \; i < \alpha\} \in V$, *then* τ *is a* P*-name.*

2.6 Exercise.

(i) Show that V^P *is a class in* V.

(ii) Show that the following ordering $<^*$ *of elements of* V^P *is well-founded:* $\tau <^* \sigma$ *if there are* $n < \omega$, $\tau_i \in V^P$, $i \leq n$, *and* $p_i \in P$, $i < n$, *such that* $\tau_0 = \tau$, $\tau_n = \sigma$ *and for all* $i < n$, $(\tau_i, p_i) \in \tau_{i+1}$.

(iii) Show that $<^*$ *is a class in* V.

2.7 Definition. *Let* G *be* P*-generic over* V.

(i) For all $\tau \in V^P$, τ_G *is defined as follows: (*$\emptyset_G = \emptyset$ *and)* $\tau_G = \{\sigma_G | \; \exists p \in G((\sigma, p) \in \tau)\}$.

(ii) $V[G] = \{\tau_G | \; \tau \in V^P\}$.

We think $V[G]$ as a $\{\in\}$-model letting the interpretation of $\in$ be the natural one that makes $V[G]$ a transitive model ($\tau_G \in^{V[G]} \sigma_G$ if $\tau_G \in \sigma_G$). We use the same notations with $V[G]$ as with V. So e.g. $\phi^{V[G]}$ denotes the sentence that says that ϕ is true in $V[G]$.

If $a \in V[G]$, then it has a name τ i.e. a P-name such that $a = \tau_G$. This name is often denoted by $\dot{a}$ (or $\hat{a}$, see below), but we are not very strict with this.

2.8 Definition. *For each* $a \in V$, *we define the standard name* $\hat{a}$ *for* a *as follows: (*$\hat{\emptyset} = \emptyset$ *and)* $\hat{a} = \{(\hat{b}, 1) | \; b \in a\}$.

2.9 Exercise. *Show that for all* P*-generic* G *over* V, $\hat{a}_G = a$ *and conclude that* $V \subseteq V[G]$.

We finish this section by defining the forcing notion $\Vdash$. In the next section we give another definition for $\Vdash$ and we prove that the two definitions are equivalent as well as the very basic properties of this notion.

We start by defining the forcing language, This is a language that works on the object side only, it does not have a counterpart on the meta side. So in the definition below we describe a sentence of the meta language that expresses what it means to be a formula in the forcing language. By a forcing language we mean the first-order logic in the vocabulary $\{\in\} \cup \{\tau | \; \tau \in V^P\}$, where the P-names τ are considered as constants. When we write a formula of this forcing language, we usually point out what are the constants. So $\phi(\tau_1, ..., \tau_n)$ means a formula in which no other constants than $\tau_1, ..., \tau_n$ appear. Notice that then for a P-generic G over V, $\phi((\tau_1)_G, ..., (\tau_n)_G)$ is a $\{\in\}$-formula with parameters from $V[G]$.

2.10 Definition. *Let* $\phi(\tau_1, ..., \tau_n)$ *be a sentence in the forcing language and* $p \in P$. *We say that* p *forces* $\phi(\tau_1, ..., \tau_n)$ *and write* $p \Vdash \phi(\tau_1, ..., \tau_n)$ *(or, if needed,* $p \Vdash_P \phi(\tau_1, ..., \tau_n)$*), if for all* P*-generic* G *over* V, *the following holds: If* $p \in G$, *then* $V[G] \models \phi((\tau_1)_G, ..., (\tau_n)_G)$.

2.11 Exercise.
(i) Suppose $p \Vdash \phi$ *and* $q \le p$*. Show that* $q \Vdash \phi$*.*
(ii) Show that $p \Vdash \phi \wedge \psi$ *iff* $p \Vdash \phi$ *and* $p \Vdash \psi$*.*
(iii) Suppose $p \Vdash \phi$ *and* $\vdash \phi \to \psi$*. Show that* $p \Vdash \psi$*.*

By $\dot{G}$ we denote the P-name $\{(\hat{p}, p) |\ p \in P\}$.

2.12 Exercise. *Show that* $\dot{G}_G = G$ *and conclude that* $G \in V[G]$*.*

3. Forcing

We define an ordering $\le^*$ to $(V^P)^2$ so that $(\tau, \sigma) \le^* (\tau', \sigma')$ if $\tau \le^* \tau'$ and $\sigma \le^* \sigma'$ (see Exercise 2.6 (ii)).

3.1 Exercise. *Show that* $\le^*$ *is well-founded.*

3.2 Definition. *For* $p \in P$ *and* P*-names* τ *and* σ*, the relation* $p \Vdash^* \tau = \sigma$ *is defined as follows:* $p \Vdash^* \tau = \sigma$ *if both (a) and (b) below hold:*

(a) for all $q \le p$ *and* $(\tau', s) \in \tau$*, if* $q \le s$*, then there are* $r \le q$ *and* $(\sigma', t) \in \sigma$ *such that* $r \le t$ *and* $r \Vdash^* \tau' = \sigma'$*.*

(b) for all $q \le p$ *and* $(\sigma', t) \in \sigma$*, if* $q \le t$*, then there are* $r \le q$ *and* $(\tau', s) \in \tau$ *such that* $r \le t$ *and* $r \Vdash^* \tau' = \sigma'$*.*

3.3 Exercise.
(i) Show that the set $\{(p, \tau, \sigma) |\ p \Vdash^* \tau = \sigma\}$ *is a class in* V*.*
(ii) Show that if for all $q \le p$ *there is* $r \le q$ *such that* $r \Vdash^* \tau = \sigma$*, then* $p \Vdash^* \tau = \sigma$*.*

3.4 Lemma. *Suppose* G *is* P*-generic over* V*.*
(i) If $p \in G$ *and* $p \Vdash^* \tau = \sigma$*, then* $\tau_G = \sigma_G$*.*
(ii) If $\tau_G = \sigma_G$*, then there is* $p \in G$ *such that* $p \Vdash^* \tau = \sigma$*.*

Proof. (i): By symmetry it is enough to show that $\tau_G \subseteq \sigma_G$. For this it is enough to show the following: If $(\tau', s) \in \tau$ and $s \in G$, then $\tau'_G \in \sigma_G$. Let $p' \in G$ be such that $p' \le p, s$. By the definition of $\Vdash^*$ and the definition of a P-generic set over V, we can find $(\sigma', t) \in \sigma$ and $r \in G$ such that $r \le p', t$ and $r \Vdash^* \tau' = \sigma'$ (exercise, hint: find a suitable dense set, the proof of (ii) may help). By the induction assumption, $\tau'_G = \sigma'_G$ and thus $\tau'_G \in \sigma_G$.

(ii): We show there is $p \in G$ such that (a) from Definition 3.2 holds. Similarly we see that there is $p \in G$ such that (b) from Definition 3.2 holds. This suffices (exercise). For a contradiction suppose that there is no such $p \in G$.

For all $p \in P$, let $q(p)$ and $(\tau'(p), s(p))$ witness the failure of (a) in the case that these elements exists. If they do not exists, we say that p is good. Now $\{q \in P |\ \exists p \in P(q \le q(p))\} \cup \{q \in P |\ q \text{ is good}\}$ is dense in P (exercise). Since we assumed that there is no good $p \in G$, there must be $p \in G$ (since G is a filter) such that $q(p) \in G$ and thus we may assume that $q(p) = p$.

But then for all $(\sigma', t) \in \sigma$ such that $t \in G$, for no $r \in G$, $r \Vdash^* \tau'(p) = \sigma'$. Thus by the induction assumption, for all $(\sigma', t) \in \sigma$ such that $t \in G$, $\tau(p)_G \ne \sigma'_G$. Since $\tau'(p)_G \in \tau_G$, we have a contradiction. □

3.5 Definition. *Suppose* $p \in P$ *and* τ *and* σ *are* P*-names. We define* $p \Vdash^* \tau \in \sigma$ *as follows:* $p \Vdash^* \tau \in \sigma$ *if for all* $q \leq p$*, there are* $r \leq q$ *and* $(\sigma', t) \in \sigma$ *such that* $r \leq t$ *and* $r \Vdash^* \tau = \sigma'$*.*

3.6 Exercise.

(i) Show that the set $\{(p, \tau, \sigma) | \, p \Vdash^* \tau \in \sigma\}$ *is a class in* V*.*

(ii) Show that if for all $q \leq p$ *there is* $r \leq q$ *such that* $r \Vdash^* \tau \in \sigma$*, then* $p \Vdash^* \tau \in \sigma$*.*

3.7 Lemma. *Suppose* G *is* P*-generic over* V*.*

(i) If $p \in G$ *and* $p \Vdash^* \tau \in \sigma$*, then* $\tau_G \in \sigma_G$*.*

(ii) If $\tau_G \in \sigma_G$*, then there is* $p \in G$ *such that* $p \Vdash^* \tau \in \sigma$*.*

Proof. As the proof of Lemma 3.4. □

3.8 Definition. *Let* $p \in P$ *and* $\phi = \phi(\tau_1, ..., \tau_n)$ *be a sentence in the forcing language. We define* $p \Vdash^* \phi$ *as follows:*

(i) If ϕ *is an atomic formula, we have already defined* $p \Vdash^* \phi$*.*

(ii) If $\phi = \neg\psi$*, then* $p \Vdash^* \phi$ *if there is no* $q \leq p$ *such that* $q \Vdash^* \psi$*.*

(iii) If $\phi = \psi \wedge \theta$*, then* $p \Vdash^* \phi$ *if* $p \Vdash^* \psi$ *and* $p \Vdash^* \theta$*.*

(iv) If $\phi = \exists v_k \psi(v_k, \tau_1, ..., \tau_n)$*, then* $p \Vdash^* \phi$ *if for all* $q \leq p$ *there are a* P*-name* τ *and* $r \leq q$ *such that* $r \Vdash^* \psi(\tau, \tau_1, ..., \tau_n)$*.*

3.9 Exercise.

(i) Show that the set $\{(p, \phi) | \, p \Vdash^* \phi\}$ *is a class in* V*.*

(ii) Show that if for all $q \leq p$ *there is* $r \leq q$ *such that* $r \Vdash^* \phi$*, then* $p \Vdash^* \phi$*.*

(iii) Show that if $p \Vdash^* \phi$ *and* $q \leq p$*, then* $q \Vdash^* \phi$*.*

3.10 Theorem. *Suppose* G *is* P*-generic over* V*.*

(i) If $p \in G$ *and* $p \Vdash^* \phi(\tau_1, ..., \tau_n)$*, then* $V[G] \models \phi((\tau_1)_G, ..., (\tau_n)_G)$*.*

(ii) If $V[G] \models \phi((\tau_1)_G, ..., (\tau_n)_G)$*, then for some* $p \in G$*,* $p \Vdash^* \phi(\tau_1, ..., \tau_n)$*.*

Proof. We prove the claims simultaneously by induction on ϕ. If ϕ is an atomic formula, then we have already proved this. We prove the claims in the case $\phi = \neg\psi$, the two other cases are left as an exercise.

(i): For a contradiction suppose $V[G] \models \psi$. Then by the induction assumption, there is $q \in G$ such that $q \Vdash^* \psi$. By Exercise 3.9, we may assume that $q \leq p$, a contradiction.

(ii): For a contradiction, suppose that there is no such $p \in G$ i.e. for all $p \in G$ there is $q_p \in P$ such that $q_p \leq p$ and $q_p \Vdash^* \psi$. But then as in the proof of Lemma 3.4, we can find $p \in G$ such that $q_p \in G$. By the induction assumption $V[G] \models \psi$, a contradiction. □

3.11 Corollary. $p \Vdash \phi$ *iff* $p \Vdash^* \phi$*.*

Proof. From right to left the claim follows immediately from Theorem 3.10 (i). For the other direction, by Exercise 3.9 (ii), it is enough to show that for all $q \leq p$, there is $r \leq q$ such that $r \Vdash^* \phi$. But this is clear by Theorem 3.10 (ii). □

We finish this section by showing that $V[G]$ satisfies all the axioms of ZFC.

3.12 Theorem. *Let ϕ be an axiom of ZFC. Then $\phi^{V[G]}$ holds.*

Proof. For extensionality, foundation and infinity, the claim is immediate by our construction of $V[G]$. We prove separation, the rest are similar.

Let τ and $\tau_1, ..., \tau_n$ be P-names and $\phi(v_0, ..., v_n)$ be a formula. Let G be P-generic over V. We need to show that the set

$$a = \{x \in \tau_G |\ \phi(x, (\tau_1)_G, ..., (\tau_n)_G)^{V[G]}\}$$

is in $V[G]$. For this we need to find a P-name for a.

We let σ be the set of all pairs (δ, p) such that

(i) $p \in P$ and for some $q \geq p$, $(\delta, q) \in \tau$,

(ii) $p \Vdash \phi(\delta, \tau_1, ..., \tau_n)$.

Notice that by Exercise 3.9 (i), σ is a P-name (i.e. is in V). We are left to show that $\sigma_G = a$.

$\sigma_G \subseteq a$: Suppose $\delta'_G \in \sigma_G$. Then there are $p \in G$ and δ such that $(\delta, p) \in \sigma$ and $p \Vdash \delta' = \delta$. But then $\delta'_G = \delta_G \in \tau_G$ and $\phi(\delta_G, (\tau_1)_G, ..., (\tau_n)_G)^{V[G]}$ holds i.e. $\delta'_G \in a$.

$a \subseteq \sigma_G$: Suppose $\delta'_G \in a$. Then $\delta'_G \in \tau_G$ and so there are $p \in G$ and δ such that $p \Vdash \delta' = \delta$ and $(\delta, q) \in \tau$ for some $q \geq p$. Also for some $p' \in G$, $p' \Vdash \phi(\delta', \tau_1, ..., \tau_n)$. Clearly we may assume that $p' = p$. But then by Exercise 2.11, $p \Vdash \phi(\delta, \tau_1, ..., \tau_n)$ and thus $\delta_G \in \sigma_G$ and so also $\delta'_G \in \sigma_G$. □

3.13 Exercise. *Show that the pairing axiom is true in $V[G]$.*

3.14 Exercise.

(i) Show that if $p \Vdash \exists v_k \psi(v_k, \tau_1, ..., \tau_n)$, then there is a P-name τ such that $p \Vdash \psi(\tau, \tau_1, ..., \tau_n)$. Hint: Definition 4.1 and Exercise 4.2 below.

(ii) Suppose $C \in V[G]$ is a set of P-names. Show that in $V[G]$ there is a function $f : C \to V[G]$ such that for all $\tau \in C$, $f(\tau) = \tau_G$.

3.15 Lemma. *Let G be P-generic over V. Then $On^{V[G]} = On^V$.*

Proof. Clearly $On^V \subseteq On^{V[G]}$. So for a contradiction, suppose that there is $\alpha \in On^{V[G]}$ such that $\alpha \notin On^V$. Then $On^V \subseteq \alpha$. Let τ be a P-name such that $\tau_G = \alpha$ and let A be the set of all P-names σ such that $(\sigma, q) \in \tau$ for some $q \in P$. Let $\kappa \in V$ be a cardinal for which there is a bijection $f : A \times P \to \kappa$ (in V). Let κ^+ be the successor of κ in V.

Then there is some $p \in P$ such that $p \Vdash \widehat{\kappa^+} \subseteq \tau$. And so for all $\gamma \in \kappa^+$ there is $(\delta_\gamma, p_\gamma) \in A \times P$ such that $p_\gamma \Vdash \delta_\gamma = \hat{\gamma}$. By Corollary 3.11 and Exercise 3.9 (i), we can choose δ_γ and p_γ so that the function $g : \kappa^+ \to A \times P$, $g(\gamma) = (\delta_\gamma, p_\gamma)$ is in V and clearly it is an injection. Thus $f \circ g$ is an injection from κ^+ to κ, a contradiction. □

4. Negation of continuum hypothesis

In this section we prove the consistency of the negation of the continuum hypothesis.

4.1 Definition. *Let $P = (P, <)$ be a partial order.*

(i) We say that $A \subseteq P$ is an antichain if for all $p, q \in A$, if $p \neq q$, then $p \perp q$. We say that A is a maximal antichain if no antichain is a proper extension of A.

(ii) For a cardinal κ, we say that P has κ-cc (chain condition) if $|A| < \kappa$ for all antichains $A \subseteq P$.

4.2 Exercise.

(i) Suppose $A \subseteq P$ is an antichain (in V). Show that A is maximal iff $D = \{p \in P | \ \exists q \in A(p \leq q)\}$ is dense in P.

(ii) Show that if $A \subseteq P$ is a maximal antichain (in V) and G is P-generic over V, then $G \cap A$ is a singleton.

Recall that by ω_1 we denote the least cardinal $> \omega$ i.e. ω^+. ω_1-cc is usually called ccc (countable chain condition).

4.3 Theorem. *Suppose that in V the following holds: P has κ-cc and $cf(\lambda) = \gamma \geq \kappa$. Let G be P-generic over V. Then in $V[G]$, $cf(\lambda) = \gamma$.*

Proof. For a contradiction, suppose that in $V[G]$ there are $\theta < \gamma$ and $f : \theta \to \lambda$ such that $\cup(rng(f)) = \lambda$ (notice that since $\gamma \subseteq V$, $\theta \in V$). Let $\dot{f}$ be a P-name such that $\dot{f}_G = f$. When this happens, we say that $\dot{f}$ is a P-name for f.

4.3.1 Exercise. *Show that there is a P-name τ and $p \in G$ such that $p \Vdash \tau = \dot{f}$ and 1 forces that τ is a function from $\hat{\theta}$ to $\hat{\lambda}$.*

So we may assume that 1 forces that $\dot{f}$ is a function from $\hat{\theta}$ to $\hat{\lambda}$.

4.3.2 Exercise. *Show that for all $\alpha < \theta$, there is a maximal antichain $A_\alpha \subseteq P$ such that for all $p \in A_\alpha$, there is β_p for which $p \Vdash \dot{f}(\hat{\alpha}) = \hat{\beta}_p$.*

For all $\alpha < \theta$, let $\delta_\alpha = \cup\{\beta_p + 1 | \ p \in A_\alpha\}$. By κ-cc and the assumption that $cf(\lambda) \geq \kappa$, $\delta_\alpha < \lambda$. Let $\delta = \cup\{\delta_\alpha | \ \alpha < \theta\}$. Since $\theta < cf(\lambda)$, $\delta < \lambda$. But clearly, $rng(f) \subseteq \delta$, a contradiction. $\square$

4.4 Corollary. *If in V, P has κ-cc, κ is regular and $\lambda \geq \kappa$ is a cardinal, then λ is a cardinal also in $V[G]$.*

Proof. Clearly it is enough to prove this under the additional assumption that λ is regular (exercise). But then the claim follows immediately from Theorem 4.3. $\square$

Theorem 4.3 gives an alternative way of proving Lemma 3.15.

4.5 Corollary. *Suppose in V, P is a partial order and G is P-generic over V. Then for all $\alpha \in V[G]$, $(\alpha \in On)^{V[G]}$ iff $\alpha \in V$ and $(\alpha \in On)^V$.*

Proof. By Exercise 2.2 (ii), it is enough to show that $(\alpha \in On)^{V[G]}$ implies that $\alpha \in V$. For this it is enough to find a cardinal $\lambda \in V$ such that in $V[G]$, $\alpha < \lambda$ (as above). Let $\dot{\alpha}$ be such that $\dot{\alpha}_G = \alpha$. Then there are (in V) a cardinal κ and a function f such that $dom(f) = \kappa$ and

$$rng(f) = \{\tau \in TC(\dot{\alpha}) | \ \exists p \in P((\tau, p) \in \dot{\alpha})\}.$$

Now in V, choose a regular cardinal λ so that $\lambda > \kappa$ and $\lambda > |P|$. Then By Corollary 4.4, λ is a cardinal also in $V[G]$. Also by Exercise 3.14, in $V[G]$, there is a function g such that $dom(g) = \kappa$ and for all $\gamma < \kappa$, $g(\gamma) = f(\gamma)_G$. Then clearly $\alpha \subseteq rng(g)$ and thus $|a| < \lambda$. But then $\alpha < \lambda$. □

4.6 Definition. *Let $\kappa > \omega$ be a regular cardinal.*

(i) $C \subseteq \kappa$ is called cub (closed and unbounded) if it is unbounded in κ (i.e. for all $\alpha < \kappa$ there is $\beta \in C$ such that $\beta > \alpha$) and for all $\alpha < \kappa$, if $\cup(C \cap \alpha) = \alpha$, then $\alpha \in C$.

(ii) $S \subseteq \kappa$ is stationary if for all cub $C \subseteq \kappa$, $S \cap C \neq \emptyset$.

4.7 Exercise. *Suppose that for all $\alpha < \kappa$, $C_\alpha \subseteq \kappa$ is cub. Show that*

$$\Delta_{\alpha<\kappa} C_\alpha = \{\alpha \in \kappa |\ \forall \gamma < \alpha(\alpha \in C_\gamma)\}$$

is cub. Conclude that every cub set is stationary.

4.8 Lemma. *(Fodor's lemma) Suppose $S \subseteq \kappa$ is stationary and $f : S \to \kappa$ is such that for all $\alpha \in S$, $f(\alpha) < \alpha$. Then there is a stationary $S' \subseteq S$ and $\alpha < \kappa$ such that $f(\gamma) = \alpha$ for all $\gamma \in S'$.*

Proof. Suppose that there are no such S' and α. Then for all $\alpha < \kappa$, there is cub $C_\alpha \subseteq \kappa$ such that for all $\gamma \in C_\alpha \cap S$, $f(\gamma) \neq \alpha$. Let $\gamma \in (\Delta_{\alpha<\kappa} C_\alpha) \cap S$. Then for all $\alpha < \gamma$, $f(\gamma) \neq \alpha$, a contradiction. □

Recall that by $|\alpha|^{<\kappa}$ we mean the cardinality of the set $\{f : \beta \to |\alpha| \mid \beta < \kappa\}$ which is the same as the cardinality of the set $\{f : \beta \to \alpha |\ \beta < \kappa\}$.

4.9 Lemma. *(Δ-lemma) Suppose $\lambda > \kappa$ are regular cardinals, for all $\alpha < \lambda$, $|\alpha|^{<\kappa} < \lambda$ and A be a set. For all $i < \lambda$, let $A_i \subseteq A$ be a set of size $< \kappa$. Then there is an unbounded $X \subseteq \lambda$ and $Y \subseteq A$ such that for all $i, j \in X$, if $i \neq j$, then $A_i \cap A_j = Y$.*

Proof. Without loss of generality we may assume that $A = \lambda$. Let $S = \{\gamma < \lambda |\ cf(\gamma) = \kappa\}$.

4.9.1 Exercise. *Show that S is stationary.*

Define $f : S \to \lambda$ so that $f(\gamma) = \cup(A_\gamma \cap \gamma)$. Notice that for all $\gamma \in S$, $f(\gamma) < \gamma$. By Fodor's lemma, there is stationary $S' \subseteq S$ and $\alpha < \lambda$ such that $f(\gamma) = \alpha$ for all $\gamma \in S'$. By the pigeon hole principle and the assumption that $|\alpha + 1|^{<\kappa} < \lambda$, there is $Y \subseteq (\alpha + 1)$ and unbounded $X' \subseteq S'$ such that for all $\gamma \in X'$, $A_\gamma \cap \gamma = Y$.

By induction on $i < \lambda$, we choose ordinals $\gamma_i \in X'$ as follows:

(i) $\gamma_0 = min(X' - \alpha)$,

(ii) for $i > 0$, $\gamma_i = min(X' - \cup\{(\gamma_j \cup \bigcup A_{\gamma_j}) + 1 |\ j < i\})$.

Then Y and $X = \{\gamma_i |\ i < \lambda\}$ are as wanted. □

4.10 Definition. *By CH (continuum hypothesis) we mean the claim $2^\omega = \omega_1$.*

Now we are ready to prove the consistency the the negation of continuum hypothesis. We present the proof the way forcing constructions are usually presented and in the next section we study the reason why the proof shows the claim (and what it is that we claim).

4.11 Theorem. *(Cohen) Con(ZFC) implies Con(ZFC+$\neg$CH)*

Proof. In V, let κ be a cardinal $> \omega_1$ and P be the partial order of all functions $p : X_p \to 2$, $X_p \subseteq \kappa \times \omega$ finite, ordered by inverse inclusion i.e. $p \le q$ if $q \subseteq p$.

4.11.1 Exercise. *Show that (in V) P has ccc. Hint: Suppose that $\{p_i \mid i < \omega_1\}$ is an antichain and start by applying Δ-lemma to the set $\{X_{p_i} \mid i < \omega_1\}$.*

Let G be P-generic over V and then from $V[G]$ we find the function $F = \cup G : \kappa \times \omega \to 2$ and sets $X_\alpha = \{n < \omega \mid F(\alpha, n) = 1\}$, $\alpha < \kappa$.

4.11.2 Exercise.
(i) Show that, indeed, dom$(\cup G) = \kappa \times \omega$.
(ii) Show that for all $\alpha < \beta < \kappa$, $X_\alpha \neq X_\beta$.

By Corollaries 4.4 and 4.5, V and $V[G]$ have the same cardinals and thus in $V[G]$, $2^\omega \ge \kappa > \omega_1$. □

5. Why forcing works

The proof of Theorem 4.11 shows that if, on the meta level, there is a proof of CH from ZFC, then on the meta level there is a proof of contradiction from ZFC (and in fact there is a mechanical method of forming a proof of contradiction from any proof of CH, making the forcing a constructive method). The reason for this is the following:

So suppose that we are given a proof $\mathcal{D}$ of CH from ZFC. Let T be the finite set of axioms of ZFC used in the proof $\mathcal{D}$. Then, by looking at the proofs of Theorems 3.12 and 4.11, one can can find a finite set T^* of axioms of ZFC such that ZFC$\cup\{\phi^V \mid \phi \in T^*\} \cup \{$"$V$ is countable and transitive"$\}$ proves $\psi^{V[G]}$ for every $\psi \in T \cup \{\neg\text{CH}\}$. Now using vakioiden lemma from the course Matemaattinen logiikka, we get that ZFC proves

$$\text{"}\forall V((\text{"}V \text{ is countable and transitive"} \wedge \bigwedge_{\phi \in T^*} \phi^V) \to (\bigwedge_{\psi \in T \cup \{\neg \text{CH}\}} \psi^{V[G]}))\text{"}.$$

5.1 Fact. *([Ku]) For all finite $T' \subseteq ZFC$, ZFC proves that there exists countable and transitive V such that for all $\phi \in T'$, ϕ^V holds.*

Thus by Fact 5.1, ZFC proves that there exists V^* such that for all $\phi \in T \cup \{\neg\text{CH}\}$, ϕ^{V^*} holds.

On the other hand, since T proves CH, ZFC proves that "$T \vdash$ CH" (as in the proof of Gödel's second incompleteness theorem in the course Matemaattinen logiikka). Since ZFC also proves soundness (korrektisuuslause in the course Matemaattinen logiikka), ZFC proves CH^{V^*}. Thus ZFC proves that there is V^* in which a contradiction holds. As we saw in the course Matemaattinen logiikka, ZFC also proves that there is no V^* which satisfies a contradiction and thus we have a proof of a contradiction from ZFC.

5.2 Exercise. *Does the proof of Theorem 4.11 show that ZFC+"$ZFC \vdash CH$" is inconsistent?*

5.3 Exercise. *What is wrong in the following deduction: By Fact 5.1, for every finite subset T of ZFC, ZFC proves that T has a model. ZFC also proves the compactness theorem, in particular, it proves that if every finite subset T of ZFC has a model then ZFC has a model. Thus ZFC proves that ZFC has a model.*

6. Continuum hypothesis

In this section we prove the consistency of CH. Originally this was proved by Gödel. He did this by showing that CH is true in the universe of constructible sets. This method is still used a lot to prove consistency results but often these results can be proved also by using forcing. Consistency of CH is one such results.

6.1 Definition. *We say that partial order P is κ-closed if for all $\alpha < \kappa$ and all $p_i \in P$, $i < \alpha$, the following holds: If for all $i < j < \alpha$, $p_j \le p_i$, then there is $p \in P$ such that $p \le p_i$ for all $i < \alpha$.*

6.2 Theorem. *Suppose P is κ-closed, G is P-generic over V, $X \in V$, $Y \in V[G]$, $Y \subseteq X$ and in $V[G]$, $|Y| < \kappa$. Then $Y \in V$.*

Notice that above we do not yet know that κ is a cardinal in $V[G]$.

Proof. So in $V[G]$, there is $\lambda < \kappa$ and $f : \lambda \to X$ such that $Y = rng(f)$ and let $\dot{f}$, $\dot{Y}$ and $\hat{A}$ be P-names for f, Y and $A = P(X)^V \in V$. Then there is $p \in P$ which forces that $\dot{Y} = rng(\dot{f})$ and $dom(\dot{f}) = \hat{\lambda}$ and $\dot{Y} \notin \hat{A}$ and $\dot{Y} \subseteq \hat{X}$.

For all $\gamma \le \lambda$, we construct $p_\gamma \in P$ and $x_{\gamma+1} \in X$ as follows:

(i) $p_0 = p$,

(ii) $p_{\gamma+1}$ is such that $p_{\gamma+1} \le p_\gamma$ and for some $x_{\gamma+1} \in X$, $p_{\gamma+1}$ forces that $\dot{f}(\hat{\gamma}) = \hat{x_{\gamma+1}}$,

(iii) if γ is a limit ordinal, then p_γ is any element of P such that $p_\gamma \le p_i$ for all $i < \gamma$.

Let $Z = \{x_{\gamma+1} | \gamma < \lambda\} \in V$. Then p_λ forces that $rng(\dot{f}) = \hat{Z} \in \hat{A}$, a contradiction. □

6.3 Exercise. *Suppose P is κ-closed, $\lambda \le \kappa$ is a cardinal (in V) and G is P-generic over V. Show that λ is a cardinal in $V[G]$.*

6.4 Theorem. *Con(ZFC) implies Con(ZFC+CH).*

Proof. Let $\kappa = 2^\omega$ and let P be the set of all functions $f : \alpha \to \kappa$, $\alpha < \omega_1$, ordered by the inverse inclusion. Clearly P is ω_1-closed. Let G be P-generic over V and $f = \cup G \in V[G]$.

6.4.1 Exercise. *Show that f is a surjection from $(\omega_1)^V$ onto κ.*

By Theorem 6.2, in $V[G]$ there are no new subsets of ω and thus $P(\omega)^V = P(\omega)^{V[G]}$. Also by Exercise 6.3, $(\omega_1)^V = (\omega_1)^{V[G]}$ and so, in $V[G]$, $|P(\omega)| \le \omega_1$ and thus CH holds. □

6.5 Exercise. *Prove the consistency of the following claims:*
(i) $2^\omega = \omega_1$ *and* $2^{\omega_1} = \omega_2$,
(ii) $2^\omega = 2^{\omega_1} = \omega_2$,
(iii) $2^\omega = \omega_1$ *and* $2^{\omega_1} > \omega_2$.

7. Iterated forcing - the starting point

In forcing, finding a suitable partial order is the main difficulty (keeping in mind that one also has to show that the partial order works). From the literature one can find several methods that are developed to help one to find these partial orders. The most used method is iterated forcing. We start by going back to Exercise 6.5 and do the constructions in a very complicated way. This helps in the next section.

In iterations the requirement that the partial order $P = (P, \le, 1)$ must satisfy that $p \le q$ and $q \le p$ implies that $p = q$, causes technical inconveniences. Thus we lift this requirement i.e. we require only that $\le$ is transitive and reflexive. Then pEq if $p \le q$ and $q \le p$ is an equivalence relation and P/E is a partial order in the old sense when one defines $p/E \le q/E$ if $p \le q$ and P and P/E work in forcing exactly the same way (exercise). And if one wants, one can replace all partial orders P with P/E everywhere below.

Thoughout this section $P = (P, \le, 1)$ is a partial order (in V and in our new sense).

7.1 Definition.

(i) We say that $Q = (\dot{Q}, \dot{\le}, \dot{1}) = (Q, \le, 1)$ *is a* P*-name of a partial order if* $\dot{Q}$, $\dot{\le}$ *and* $\dot{1}$ *are* P*-names and* 1 *forces that* $\dot{\le}$ *is a partial order of* $\dot{Q}$ *with the largest element* $\dot{1}$ *and* $(\dot{1}, 1) \in Q$. *We will write* Q *for* $\dot{Q}$ *etc. It should be clear from the context what we mean.*

(ii) $P \star Q$ *is the set*

$$\{(p,\tau) |\ p \in P,\ \exists q \in P((\tau, q) \in Q),\ p \Vdash \tau \in Q\}$$

ordered by the following partial order: $(p,\tau) \le (q,\sigma)$ *if* $p \le q$ *and* $p \Vdash \tau \le \sigma$. *(The largest element is* $(1,1)$*.) The set of those* P*-names* τ *for which there is* $p \in P$ *such that* $(\tau, p) \in Q$ *is denoted by* $Dom(Q)$.

(iii) $i : P \to P \star Q$ *is the function* $i(p) = (p, 1)$.

From now on we let Q be a P-name for a partial order and i as in Definition 7.1 (iii).

7.2 Exercise. i *is a complete embedding (see [Ku]), in particular,*
(i) if $p, q \in P$ *and* $p \le q$, *then* $i(p) \le i(q)$,
(ii) if $p, q \in P$, *then* $p \perp q$ *iff* $i(p) \perp i(q)$,
(iii) if $(p,\tau) \in P \star Q$ *and* $q \le p$, *then* $(p,\tau) || i(q)$.

7.3 Exercise. *Suppose K is $P\star Q$-generic over V. Show that $K_P = i^{-1}(K)$ is P-generic over V. Hint: Use Exercise 7.2.*

7.4 Definition.

(i) If G is a P-generic over V and $H \subseteq Q_G$, then $G\star H$ is the set of those $(p,\tau)\in P\star Q$ such that $p\in G$ and $\tau_G\in H$.

(ii) If K is $P\star Q$-generic over V and $G = K_P$, then K_Q is the set of those τ_G such that for some $q\in P$, $(q,\tau)\in K$.

7.5 Lemma. *Suppose K is $P\star Q$-generic over V, $G = K_P$ and $H = K_Q$. Then H is Q_G-generic over $V[G]$, $K = G\star H$ and $V[K] = V[G][H]$.*

Proof. H is Q_G-generic over $V[G]$: The proof that H is a filter is left as an exercise and so we prove only that H is generic. For this let δ be a P-name for a dense subset of Q_G i.e. some $p\in G$ forces that δ is a dense subset of Q. But then $D = \{(q,\tau)\in P\star Q|\ q\le p,\ q\Vdash \tau\in\delta\}\cup\{(q,\tau)\in P\star Q|\ q\perp p\}$ is dense in $P\star Q$ (exercise). Thus there is $(q,\tau)\in K\cap D$. Since K is a filter, $q||p$ and so $\tau_G\in\delta_G\cap H$.

$K = G\star H$: The direction $\subseteq$ is immediate by the definitions and so we prove only that $G\star H\subseteq K$: So suppose $(p,\tau)\in G\star H$. Then $p\in G$ i.e. $(p,1)\in K$ and $\tau_G\in H$ i.e. for some $q\in P$, $(q,\tau)\in K$ (and p forces that $\tau\in Q$ since $G\star H\subseteq P\star Q$). Since K is a filter there is some $(r,\rho)\in K$ such that $(r,\rho)\le(p,1),(q,\tau)$. But then $(r,\rho)\le(p,\tau)$ and so $(p,\tau)\in K$.

$V[K] = V[G][H]$ is left as an exercise. (Hint: Show first that $K\in V[G][H]$ and $G,H\in V[K]$.) □

7.6 Exercise. *Suppose G is P-generic over V and H is Q_G-generic over $V[G]$. Then $G\star H$ is $P\star Q$-generic over V.*

7.7 Exercise. *Suppose P has ccc, $X\in V$ and τ is a P-name of which 1 forces that $\tau\subseteq\hat{X}$ and that τ is countable. Show that there exists a countable $Y\subseteq X$ in V such that $1\Vdash\tau\subseteq\hat{Y}$. Hint: Choose a P-name $\dot{f}$ such that 1 forces that $\dot{f}$ is a function from $\hat{\omega}$ onto τ and repeat the argument from the proof of Theorem 4.3.*

7.8 Lemma. *If P has ccc and 1 forces that Q has ccc, then $P\star Q$ has ccc.*

Proof. For a contradiction, suppose $\{(p_i,\tau_i)\in P\star Q|\ i<\omega_1\}$ is an antichain. Let $\delta = \{(\hat{p_i},p_i)|\ i<\omega_1\}$.

7.8.1 Exercise. *Show that if G is P-generic over V, then δ_G is a countable subset of P in $V[G]$. Hint: Any two elements of δ_G are compatible.*

Thus by Exercise 7.7, there is countable $Y\subseteq P$ such that $1\Vdash\delta\subseteq\hat{Y}$. But since for all $i<\omega_1$, $p_i\Vdash\hat{p_i}\in\delta$, the set $\{p_i|\ i<\omega_1\}$ is countable. Thus there is an uncountable set $X\subseteq\omega_1$ such that for all $i,j\in X$, $p_i = p_j = p$. Since 1 forces that Q has ccc, there are $q\le p$ and $i,j\in X$, $i\ne j$, such that $q\Vdash\tau_i||\tau_j$. But then $(p_i,\tau_i)||(p_j,\tau_j)$, a contradiction. □

8. Finite support iteration

Now we are ready to define finite support iterations:

8.1 Definition. *We say that* $(P_\gamma, Q_\gamma)_{\gamma\le\alpha}$ *is a finite support iteration if the following holds:*

(i) P_0 *is the one element partial order* $\{\emptyset\}$.

(ii) $Q_\gamma = (Q_\gamma, \le, 1)$ *is a* P_γ*-name for a partial order.*

(iii) $P_{\gamma+1}$ *is the set of all functions* p *with domain* $\gamma+1$ *such that* $p\restriction\gamma \in P_\gamma$ *and* $\tau = p(\gamma)$ *is such that for some* $q\in P_\gamma$, $(\tau, q)\in Q_\gamma$ *and* $p\restriction\gamma \Vdash \tau\in Q_\gamma$. $P_{\gamma+1}$ *is ordered so that* $p\le q$ *if* $p\restriction\gamma \le q\restriction\gamma$ *and* $p\restriction\gamma\Vdash p(\gamma)\le q(\gamma)$. *(Notice that then* $P_{\gamma+1}$ *is isomorphic with* $P_\gamma \star Q_\gamma$*.)*

(iv) For limit γ, P_γ *is the set of all functions* p *with domain* γ *such that for all* $\beta<\gamma$, $p\restriction\beta\in P_\beta$ *and the support*

$$supp(p) = \{\beta < dom(p) |\ p(\beta)\ne 1\}$$

is finite. P_γ *is ordered so that* $p\le q$ *if for all* $\beta<\gamma$, $p\restriction\beta\le q\restriction\beta$.

From now on, $(P_\gamma, Q_\gamma)_{\gamma\le\alpha}$ is a finite support iteration. Notice that Q_α does not play a role in the definition of P_α (it is there for notational reasons).

8.2 Definition. *For* $\gamma\le\beta\le\alpha$, *by* $i_{\gamma\beta}$ *we mean the function from* P_γ *to* P_β *such that for all* $p\in P_\gamma$, $i_{\gamma\beta}(p)$ *is the element* $q\in P_\beta$ *for which* $q\restriction\gamma = p$ *and for all* $\delta\in\beta-\gamma$, $q(\delta)=1$.

8.3 Exercise. *Suppose* $\gamma\le\beta\le\alpha$, $p, p'\in P_\gamma$ *and* $q, q'\in P_\beta$.

(i) If $q\le q'$, *then* $q\restriction\gamma, q'\restriction\gamma\in P_\gamma$ *and* $q\restriction\gamma\le q'\restriction\gamma$.

(ii) If $p\le p'$, *then* $i_{\gamma\beta}(p)\le i_{\gamma\beta}(p')$.

(iii) If $q\restriction\gamma\perp q'\restriction\gamma$, *then* $q\perp q'$.

(iv) If $supp(q)\cap supp(q')\subseteq\gamma$, *then* $q\perp q'$ *iff* $q\restriction\gamma\perp q'\restriction\gamma$.

(v) $p\perp p'$ *iff* $i_{\gamma\beta}(p)\perp i_{\gamma\beta}(p')$.

(vi) Suppose $p = q\restriction\gamma$ *and* $p'\le p$. *Show that* $r = (q-p)\cup p'\in P_\beta$ *and* $r\le q$.

8.4 Corollary. *Suppose* $\gamma<\beta\le\alpha$, G *is* P_β*-generic over* V *and* $G' = i^{-1}_{\gamma\beta}(G)$. *Then* G' *is* P_γ*-generic over* V.

Proof. As in the previous section. □.

8.5 Exercise. *Suppose that for all* $\gamma<\alpha$, 1 *forces that* Q_γ *has ccc. Show that* P_α *has ccc. Hint: Prove by induction on* $\beta\le\alpha$ *that* P_β *has ccc. The successor steps follow immediately from Lemma 7.8 and for limit cases, make a counter assumption and use Exercise 8.3 (iv) and (in the case* $cf(\beta)=\omega_1$*)* Δ*-lemma for the supports of the elements in the antichain.*

8.6 Definition. *Let* $\gamma<\alpha$ *and* G *be* P_γ*-generic over* V. *By* P^γ_G *we mean the set of all functions* p *with domain* $\alpha-\gamma$ *such that for some* $q\in G$, $q\cup p\in P_\alpha$. *We partially order* P^γ_G *so that* $p\le p'$ *if there is some* $q\in G$, $q\cup p, q\cup p'\in P_\alpha$ *and* $q\cup p\le q\cup p'$

By P^γ *we mean a* P_γ*-name* $(\dot{P^\gamma}, \dot{\leq}, \dot{1})$ *for a partial order so that for all* P_γ*-generic* G *over* V, $(P^\gamma)_G = P^\gamma_G$ *(exists by Exercise 3.14 (i)). We may always choose* $\dot{P^\gamma}$ *to be the set* $\{(\hat{q}, p) |\ p \in P_\gamma,\ dom(q) = \alpha - \gamma, p \cup q \in P_\alpha\}$. *As usually, by* P^γ *we denote also* $\dot{P^\gamma}$ *etc.*

8.7 Exercise. *Suppose* $p, q \in P_\alpha$, $\gamma < \alpha$, $p_0 = p \restriction \gamma \leq q \restriction \gamma = q_0$ *and denote* $p_1 = p \restriction (\alpha - \gamma)$ *and* $q_1 = q \restriction (\alpha - \gamma)$. *Show that if* p_0 *forces that* $\hat{p_1} \leq \hat{q_1}$ *(in the ordering of* P^γ *), then* $p \leq q$.

The following lemma is not the most useful form of splitting iterated forcing into pieces but still gives some idea of what is going on and suffices for our purposes (in fact we will need only the very first claim).

8.8 Lemma. *Suppose* $\gamma < \alpha$, G *is* P_α*-generic over* V, $G_\gamma = i^{-1}_{\gamma\alpha}(K)$ *and* $G^\gamma = \{p \in P^\gamma_G |\ \exists q \in P_\gamma (q \cup p \in K)\}$. *Then* G^γ *is* P^γ_G*-generic over* $V[G_\gamma]$ *and* $V[G] = V[G_\gamma][G^\gamma]$.

Proof. This is basically the same what was done in Section 7 and as there we prove only that G^γ is P^γ_G-generic over $V[G_\gamma]$: For this, let τ be a P_γ-name such that τ_{G_γ} is a dense subset of P^γ_G. Then there is $p' \in G_\gamma$ such that it forces that τ is a dense subset of P^γ (keep in mind that $P^\gamma_{G_\gamma} = (P^\gamma)_{G_\gamma}$). As before, we may assume that $p' = 1$. Let $p \in P_\alpha$. For any $q \in P_\alpha$, we denote $q_0 = q \restriction \gamma$ and $q_1 = q \restriction (\alpha - \gamma)$. As in the proof of lemma 7.5 it is enough to find $q \leq p$ such that q_0 forces that $\hat{q_1} \in \tau$. Since p_0 forces that τ is dense in P^γ, there is δ such that p_0 forces that $\delta \leq \hat{p_1}$ and $\delta \in \tau$ (notice that p_0 forces that $\hat{p_1} \in P^\gamma$, exercise). Let H be P_γ-generic over V such that $p_0 \in H$. Then in $V[H]$ there are $r \in P^\gamma_H$ such that $\tau_H = r$. Let $s \in H$ be such that $s \cup r \in P_\alpha$ and s' such that it forces that $\delta = \hat{r}$. By Exercise 8.3 (vi), we may assume that $s = s' \leq p_0$ and then, by Exercise 8.7, $q = s \cup r$ is as wanted. □

8.9 Lemma. *Let* G *be* P_α*-generic over* V *and* $G(\gamma) = \{p(\gamma)_{G_\gamma} |\ p \in G\}$. *Then* $G(\gamma)$ *is* $(Q_\gamma)_{G_\gamma}$*-generic over* $V[G_\gamma]$.

Proof. By Corollary 8.4, $G_{\gamma+1}$ is $P_{\gamma+1}$-generic over V and by definitions, $P_{\gamma+1}$ is isomorphic with $P_\gamma \star Q_\gamma$. By checking the isomorphism and using Lemma 7.5, $G'(\gamma) = \{p(\gamma)_{G_\gamma} |\ p \in G_{\gamma+1}\}$ is $(Q_\gamma)_{G_\gamma}$-generic over $V[G_\gamma]$. But clearly $G(\gamma) = G'(\gamma)$. □

8.10 Exercise. *Suppose that* $cf(\alpha) \geq \omega_1$, *for all* $\gamma < \alpha$, 1 *forces that* Q_γ *has ccc,* $p \in P_\alpha$ *forces that* τ *is a function from* $\hat{\omega}$ *to* $\hat{\omega}$ *and* G *is* P_α*-generic over* V *such that* $p \in G$. *Show that there is* $\gamma < \alpha$ *such that* $\tau_G \in V[G_\gamma]$. *Hint: The proof of Theorem 4.3.*

9. Dominating number

As an application of iterated forcing, we look at dominating number.

9.1 Definition.

(i) For $f, g \in \omega^\omega$, *we write* $f <^* g$ *and say that* g *eventually dominates* f, *if there is* $n \in \omega$ *such that for all* $n < m < \omega$, $f(m) < g(m)$.

(ii) We let D *to be the set of all those* $A \subseteq \omega^\omega$ *such that for all* $f \in \omega^\omega$ *there is* $g \in A$ *which eventually dominates* f. *By* $\mathbf{d}$ *(dominating number) we mean* $min\{|A| \mid A \in D\}$.

9.2 Exercise.

(i) Show that $\mathbf{d} \geq \omega_1$.

(ii) Suppose that CH holds in V *and let* P *be the set of all* $p : X_p \to \omega$ *such that* $X_p \subseteq \omega_2 \times \omega$ *is finite. We partially order* P *by inverse inclusion (as before) i.e.* $p \leq q$ *if* $q \subseteq p$. *Let* G *be* P*-generic over* V. *Show that* $\mathbf{d} \geq \omega_2$ *in* $V[G]$. *Hint: The proof of Theorem 9.6 below may help.*

Dominating number is one example of so called cardinal invariants. Another example of such invariants is $Cov(M)$ i.e. the least cardinal κ for which there are meager (aka meagre aka of first category) subsets A_i, $i < \kappa$, of reals $\mathbf{R}$ such that $\bigcup_{i<\kappa} A_i = \mathbf{R}$. It is known that $Cov(M) \leq \mathbf{d}$.

9.3 Definition. *By* $P_\mathbf{d}$ *we mean the partial order* $(P_\mathbf{d}, \leq, (\emptyset, \emptyset))$, *where* $P_\mathbf{d}$ *is the set of pairs* $p = (f_p, F_p)$ *such that* $f_p : n_p \to \omega$ *for some* $n_p < \omega$ *and* F_p *is a finite set of functions from* ω *to* ω. $P_\mathbf{d}$ *is ordered so that* $p \leq q$ *if* $f_q \subseteq f_p$, $F_q \subseteq F_p$ *and for all* $n_q \leq i < n_p$ *and* $h \in F_q$, $f_p(i) > h(i)$.

9.4 Exercise.

(i) Show that $P_\mathbf{d}$ *has ccc.*

(ii) Let G *be* $P_\mathbf{d}$*-generic over* V *and* $g = \bigcup_{p \in G} f_p$. *Show that* g *is a function from* ω *to* ω.

9.5 Lemma. *Let* G *be* $P_\mathbf{d}$*-generic over* V *and* $g = \bigcup_{p \in G} f_p$. *Then for all* $h : \omega \to \omega$ *from* V, $h <^* g$.

Proof. Suppose not and let $\dot{g}$ be a $P_\mathbf{d}$-name for g (i.e. for all $P_\mathbf{d}$-generic H over V, $\dot{g}_H = \bigcup_{p \in H} f_p$). Then there are $h : \omega \to \omega$ and $p \in G$ such that p forces the negation of $\hat{h} <^* \dot{g}$. Let $q \in P_\mathbf{d}$ be such that $f_q = f_p$ and $F_q = F_p \cup \{h\}$ and let H be $P_\mathbf{d}$-generic over V such that $q \in H$. Then for all $i \geq n_p$, $h(i) < (\dot{g}_H)(i)$. Since $q \leq p$, we have a contradiction. □

9.6 Theorem. *Con(ZFC) implies Con(ZFC+*$\mathbf{d} = \omega_1 < 2^\omega$*).*

Proof. By Theorem 4.11, we may assume that $2^\omega > \omega_1$ in V. Let $(P_g, Q_\gamma)_{\gamma \leq \omega_1}$ be a finite support iteration such that for all $\gamma \leq \omega_1$, Q_γ is a P_γ-name for $(P_\mathbf{d})^{V[G_\gamma]}$ (i.e. for all P_γ-generic G over V, $(Q_\gamma)_{G_\gamma}$ satisfies in $V[G_\gamma]$ the definition of $P_\mathbf{d}$).

Let G be P_{ω_1}-generic over V. By Exercise 9.4 (i) and Lemma 7.8, P_{ω_1} has ccc and thus $(\omega_1)^V = (\omega_1)^{V[G]}$ and in $V[G]$ $2^\omega > \omega_1$ by Corollary 4.4. Thus it is enough to show that in $V[G]$, $A = \{f_\gamma \mid \gamma < \omega_1\}$, where $f_\gamma = \bigcup_{p \in G(\gamma)} f_p$, see Lemma 8.9, has the property that for all $g : \omega \to \omega$, there is $f \in A$ such that $g <^* f$. But this is clear: By Exercise 8.10, there is $\gamma < \omega_1$ such that $g \in V[G_\gamma]$. By Lemma 8.9, $G(\gamma)$ is $(Q_\gamma)_{G_\gamma}$-generic over $V[G_\gamma]$ and thus by Lemma 9.5, $g <^* f_\gamma$. □

10. Further exercises

In this section, in the form of exercises we look at how to kill stationary subsets of ω_1 by forcing (killing stationary subsets of $\kappa > \omega_1$ is much harder). Recall that by $X^{<\omega}$ we mean the set of all functions $f : n \to X$, $n < \omega$.

10.1 Definition. *Let $P = (P, \leq, 1)$ be a partial order.*

(i) $\Gamma(P)$ is a game of two players, I and II and it lasts ω rounds. At each round $n < \omega$ first I chooses some $p_n \in P$ and then II chooses $q_n \in P$. II must choose so that $q_n \leq p_n$ and in rounds $n > 0$, I must choose so that $p_n \leq q_{n-1}$. II wins if there is $q \in P$ such that for all $n < \omega$, $q \leq q_n$.

(ii) Winning strategy for I in $\Gamma(P)$ is a function $\sigma : P^{<\omega} \to P$ such that no matter how II plays I wins if at each round $n < \omega$, I chooses $\sigma(q_0, ..., q_{n-1})$.

(iii) We say that P is hopeless for II, if I has a winning strategy in $\Gamma(P)$.

10.2 Exercise. *Suppose that P is not hopeless for II and G is P-generic over V.*

(i) Suppose $X \in V$, $Y \in V[G]$, $Y \subseteq X$ and Y is countable. Show that $Y \in V$.

(ii) Show that $\omega_1^V = \omega_1^{V[G]}$.

Fix $S \subseteq \omega_1$ so that $\omega_1 - S$ is stationary (S may also be stationary). By $P(S)$ we mean the set of all strictly increasing $f : \alpha + 1 \to \omega_1$, $\alpha < \omega_1$, such that $rng(f) \cap S = \emptyset$ and for all limit $\gamma \leq \alpha$, $f(\gamma) = \cup_{\beta<\gamma} f(\beta)$ and we order $P(S)$ by inverse inclusion.

10.3 Exercise.

(i) Show that for all $f : \omega_1^{<\omega} \to \omega_1$, the set $C_f = \{\alpha < \omega_1 \mid f(\alpha^{<\omega}) \subseteq \alpha\}$ is cub.

(ii) Show that $P(S)$ is not hopeless for II. Hint: For a contradiction, suppose that σ is a winning strategy for I. Then think the case when at each round $n < \omega$, II plays so that she first chooses some $\gamma_n < \omega_1$ so that $\gamma_n > \cup rng(p_n)$ and then answers by $q_n = p_n \cup \{(dom(p_n), \gamma_n)\}$. Then apply (i) to the function $f(\gamma_0, ..., \gamma_{m-1}) = \cup rng(p_m)$, where for all $i \leq m$, $p_i = \sigma(q_0, ..., q_{i-1})$ and for all $i < m$ $q_i = p_i \cup \{(dom(p_i), \gamma_i)\}$ (if for some $i < m$, $q_i \notin P(S)$, let $f(\gamma_0, ..., \gamma_{m-1}) = 0$).

10.4 Exercise. *Let G be $P(S)$-generic over V and $C = rng(\cup G)$. Show that C is a cub subset of ω_1 and $C \cap S = \emptyset$ (i.e. S is not stationary in $V[G]$).*

In Exercise 10.4 the assumption that $\omega_1 - S$ is stationary is necessary:

10.5 Exercise. *Suppose P is a partial order, G is P-generic over V, $C \subseteq \omega_1$ is in V and $(\omega_1)^V = (\omega_1)^{V[G]}$.*

(i) Show that C is a cub subset of ω_1 in V iff C is a cub subset of ω_1 in $V[G]$.

(ii) Since it is possible that $\omega_1 - S$ is not cub, why the direction from right to left in (i) does not contradict Exercise 10.4?

References

[Ku] K. Kunen, Set Theory An Introduction to Independence Proofs, North Holland, Amsterdam, 1980.