MODELS OF SET THEORY

STEFAN GESCHKE

CONTENTS

1. First order logic and the axioms of set theory

1.1. **Syntax.** The *language $\mathcal{L}$ of set theory* is the first-order language with the binary relation-symbol $\in$. That is, the language $\mathcal{L}$ consists of the *formulas* over the alphabet $\{\wedge, \neg, \exists, (,), \in, =\} \cup \mathrm{Var}$, where Var is a countably infinite set of variables. By recursion on the length, we define what a formula is.

If x and y are variables, then $x \in y$ and $x = y$ are formulas. Such formulas are called *atomic*. If φ and ψ are formulas, then so are $\neg\varphi$ and $(\varphi \wedge \psi)$. If φ is a formula and x is a variable, then $\exists x\varphi$ is a formula, too.

We will frequently omit parentheses in a formula if this does not lead to any ambiguity. Also, we will add parentheses if this improves readability. $\forall x\varphi$ abbreviates $\neg\exists x\neg\varphi$ and $(\varphi \vee \psi)$ abbreviates $\neg(\neg\varphi \wedge \neg\psi)$. As usual, we will freely use other abbreviations like $\subseteq$, $\rightarrow$, and $\exists x \in y$ inside a formula.

Exercise 1.1. Let x and y be variables and let φ and ψ be formulas. Write out what the following abbreviations stand for:

$$x \subseteq y, \quad \varphi \rightarrow \psi, \quad \exists x \in y\varphi.$$

This obviously depends on your intuition of what formulas are supposed to mean. We discuss the meaning of formulas in Subsection 1.2. You may use all the previously defined abbreviations.

A *free occurrence* of a variable x in a formula φ is an occurence of x outside the scope of any quantifier $\exists x$. (Recall that $\forall x$ is just an abbreviation.) If x occurs freely in φ, then x is a *free variable* of φ. We write $\varphi(x_1, \ldots, x_n)$ instead of just φ in order to indicate that all the free variables of φ are listed among $x_1, \ldots, x_n$ and that the variables $x_1, \ldots, x_n$ are pairwise distinct. A *sentence* is a formula without free variables.

1.2. **Semantics.** We briefly discuss the intended meaning of formulas. A *structure* for the language of set theory is a set X together with a binary relation E. In the following, let X be a set and E a binary relation on X. Small letters from the beginning of the alphabet, possibly with index, such as $a, a_1, \ldots, a_n, b$ denote elements of X. Small letters from the end of the alphabet, possibly with index, such as $x, x_1, \ldots, x_n, y$ are typically variables of the language of set theory.

Let $\varphi(x_1, \ldots, x_n)$ be a formula. The intended meaning of $\varphi[a_1, \ldots, a_n]$ is the statement about $a_1, \ldots, a_n$ that is obtained by replacing every free occurence of x_i by a_i, $i = 1, \ldots, n$, and interpreting the symbol $=$ by actual equality and the symbol $\in$ by the relation E.

To make this precise, by recursion on the length of formulas we define whether (X, E) satisfies $\varphi[a_1, \ldots, a_n]$. We write $(X, E) \models \varphi[a_1, \ldots, a_n]$ for "(X, E) satisfies $\varphi[a_1, \ldots, a_n]$". We abbreviate $(x_1 \in x_2)[a_1, a_2]$ by $a_1 \in a_2$ and $(x_1 = x_2)[a_1, a_2]$ by $a_1 = a_2$.

(1) $(X, E) \models a_1 \in a_2$ iff $a_1 E a_2$.
(2) $(X, E) \models a_1 = a_2$ iff $a_1 = a_2$. Here the first $=$ is an element of the alphabet of the language of set theory, the second $=$ has the usual meaning.
(3) $(X, E) \models \neg\varphi[a_1, \ldots, a_n]$ iff $(X, E) \not\models \varphi[a_1, \ldots, a_n]$.
(4) $(X, E) \models (\varphi \wedge \psi)[a_1, \ldots a_n]$ iff

$$(X, E) \models \varphi[a_1, \ldots, a_n] \text{ and } (X, E) \models \psi[a_1, \ldots, a_n].$$

(5) Let $\varphi(x, y_1, \ldots, y_n)$ be a formula. Then the free variables of $\exists x\varphi$ are among $y_1, \ldots, y_n$. Hence we can write $(\exists x\varphi)[y_1, \ldots, y_n]$ instead of $\exists x\varphi$. Now

$$(X, E) \models (\exists x\varphi)[b_1, \ldots, b_n]$$

iff there is an element a of X such that

$$(X, E) \models \varphi[a, b_1, \ldots, b_n].$$

1.3. **Completeness, compactness and consistency.** A set of sentences is a *theory*. If Σ is a theory and (X, E) satisfies each of the sentences in Σ, we say that (X, E) is a *model* of Σ. Similarly, if (X, E) satisfies a sentence φ, we say that (X, E) is a *model* of φ. A sentence φ *follows* from Σ if every model of Σ is a model of φ. In this case we write $\Sigma \models \varphi$.

There is also a notion $\vdash$. $\Sigma \vdash \varphi$ means that φ is formally provable from Σ. The following statement about the connection between $\models$ and $\vdash$ is easily the most important theorem about first order logic.

Theorem 1.2 (Completeness Theorem). *If Σ is a theory and φ is a sentence, then $\Sigma \models \varphi$ iff $\Sigma \vdash \varphi$.*

We are going to use the Completeness Theorem freely, without referring to it explicitly.

Since formal proofs have a finite length, a formal proof of φ from Σ only uses finitely many sentences from Σ. Hence, using the completeness theorem, we obtain

Corollary 1.3 (Compactness Theorem). *If Σ is a theory and φ a sentence, then $\Sigma \models \varphi$ iff there is a finite theory $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \varphi$.*

A theory Σ is *consistent* if it does not lead to a contradiction, i.e., if there is no sentence φ such that both φ and $\neg\varphi$ are provable from Σ.

Corollary 1.4. *A theory Σ is consistent iff it has a model.*

Proof. Suppose Σ is not consistent. Let φ be a sentence such that both φ and $\neg\varphi$ follow from Σ. Now, if $M = (X, E)$ is a model of Σ, then $M \models \varphi$ and $M \models \neg\varphi$. But this contradicts the definition of $M \models \neg\varphi$.

Now suppose that Σ does not have a model and let φ be any sentence. Since Σ does not have a model, every model of Σ satisfies both φ and $\neg\varphi$. Hence, φ and $\neg\varphi$ both follow from Σ and thus, Σ is inconsistent. $\square$

We will frequently use

Corollary 1.5. *A theory Σ is consistent iff every finite subset of Σ has a model.*

Exercise 1.6. Give a proof of Corollary 1.5.

1.4. **Foundations of mathematics and the incompleteness theorems.** Practically all of mathematics can be formulated in the language of set theory. Hence, all one has to do in order to come up with a sound foundation of mathematics is to find a system of axioms, i.e., a theory, with the following properties:

(1) The axioms reflect our intuitive understanding of the concept "set".
(2) Practically all mathematical statements that are generally regarded as provable actually follow from the axioms.
(3) The axioms are consistent.

Note that the demands (1) and (2) are slightly vague, but there is common agreement that there is a system of axioms that satisfies (1)–(3), namely *Zermelo-Fraenkel Set Theory (ZF)* together with the *Axiom of Choice (AC, ZF+AC=ZFC)*. Since (1) and (2) are open to different interpretations, all we can say is that most mathematicians agree that ZFC is a suitable system of axioms. Even the mathematicians who are not familiar with ZFC almost never exceed the strength of ZFC in their proofs. In fact, most of mathematics can be done in far weaker systems of arithmetic.

(3) is a very precise statement. In particular, if (3) holds for a specific system of axioms, as a true mathematical statement it should be provable from the axioms. However, if the system of axioms was inconsistent, then it would prove its own consistency. It follows that a proof of (3) would actually not increase our believe in the consistency of the system of axioms.

In fact, Gödel has shown that for every system of axioms satisfying (1) and (2) (in a precise sense), (3) is not provable from the axioms. This is the Second Incompleteness Theorem.

Gödels First Incompleteness Theorem says that if ZFC (or any similar theory) is consistent, then there are sentences φ such that neither φ nor $\neg\varphi$ follow from it. Such a sentence φ is called *independent* over ZFC. The main goal of this course is to show that the Continuum Hypothesis (CH) is independent over ZFC.

1.5. **The axioms.** The axioms of ZFC are the following (we use some obvious abreviations):

(1) Set Existence.
$$\exists x(x = \emptyset)$$

(2) Extensionality.
$$\forall x\forall y(\forall z(z \in x \leftrightarrow z \in y) \to x = y)$$

(3) Foundation.
$$\forall x(x \neq \emptyset \to \exists y \in x\forall z \in x(z \notin y))$$

(4) Separation (really a scheme of axioms). For every formula $\varphi(x, y_1, \ldots, y_n)$ without a free occurrence of y,
$$\forall y_1 \ldots \forall y_n\forall z\exists y\forall x(x \in y \leftrightarrow x \in z \wedge \varphi(x, y_1, \ldots, y_n))$$
is an axiom.

(5) Pairing.
$$\forall x\forall y\exists z(x \in z \wedge y \in z)$$

(6) Union.
$$\forall F\exists A\forall Y \in F(Y \subseteq A)$$

(7) Replacement (again a scheme of axioms). For every formula $\varphi(x, y, y_1, \ldots, y_n)$, without a free occurence of y,
$$\forall y_1 \ldots \forall y_n\forall A(\forall x \in A\exists!y\varphi(x, y, y_1, \ldots, y_n)$$
$$\to \exists Y\forall x \in A\exists y \in Y\varphi(x, y, y_1, \ldots, y_n))$$
is an axiom. Here $\exists!$ means "there is exactly one".

(8) Infinity.
$$\exists x(\emptyset \in x \wedge \forall y \in x(y \cup \{y\} \in x))$$

(9) Power set.
$$\forall x\exists y\forall z(z \subseteq x \to z \in y)$$

(10) Choice.
$$\forall x\exists R(R \text{ is a well-ordering of } x)$$

For the Axiom of Choice recall that a binary relation $\leq$ on a set X is well-ordering if $\leq$ is a linear order on X and every non-empty set $Y \subseteq X$ has a minimal element with respect to $\leq$. (See also Definition .)

Exercise 1.7. Write out the formulas $\exists!x\varphi$, $x = \emptyset$, and $x = y \cup z$.

Exercise 1.8. Write out the formula "R is a well-ordering of x".

Note that since Separation and Replacement are schemes and not just single axioms, ZFC consists of infinitely many axioms.

2. Review of basic set theory

2.1. **Classes.** Assume that we live in a universe of sets that satisfies all the axioms of ZFC. This is the usual framework in which mathematics takes place. A class C is a collection of all sets with a certain property. More precisely, if $\varphi(x, y_1, \ldots, y_n)$ is a formula and $b_1, \ldots, b_n$ are sets, then $C = \{a : \varphi[a, b_1, \ldots, b_n]\}$ is a class, the class defined by $\varphi(x, y_1, \ldots, y_n)$ and the parameters $b_1, \ldots, b_n$. The class $C = \{a : \varphi[a, b_1, \ldots, b_n]\}$ is identified with a set c iff $\varphi[a, b_1, \ldots, b_n]$ is equivalent to $a \in c$. A class that does not correspond to a set in this way is a *proper class.*

We now consider the same situation, but inside a structure $M = (X, E)$ for the language of set theory that we can look at from the outside. The variables of our language range over elements of the structure, i.e., they are interpreted by elements of the structure, the sets of M. If $b_1, \ldots, b_n$ are elements of X and $\varphi(x, y_1, \ldots, y_n)$ is a formula, then $C = \{a \in X : M \models \varphi[a, b_1, \ldots, b_n]\}$ is a class of M, the *class defined by the formula $\varphi(x, y_1, \ldots, y_n)$* with the *parameters $b_1, \ldots, b_n$.* Note that looking at M from the outside, C is a set.

C can correspond to an element of X in the following way: It might happen that for some $c \in X$ we have that for all $a \in M$,

$$M \models a \in c \quad \Leftrightarrow \quad M \models \varphi[a, b_1, \ldots, b_n],$$

i.e., $C = \{a \in X : aEc\}$. This is the situation in which we identify C with c. If R is a binary relation and b is a set, then $\mathrm{ext}_R(b) = \{a : aRb\}$ is the *extension* of b with respect to R or the *R-extension* of b. Note that the Axiom of Extensionality just says that two sets are the same iff they have the same $\in$-extension. This can be written as $\forall x (\mathrm{ext}_\in(x) = x)$. In other words, every set is uniquely determined by its $\in$-extension.

The most important class is V, the class of all sets. V is a proper class. We will soon define other important proper classes.

2.2. **Well-founded relations and recursion.** Let C be a class and R a binary relation on C. R is *set-like* if for all $a \in C$, $\mathrm{ext}_R(a)$ is a set. R is *well-founded* if every non-empty subset S of C has an R-minimal element, i.e., there is $a \in S$ such that $S \cap \mathrm{ext}_R(a) = \emptyset$.

The Axiom of Foundation says that $\in$ is well-founded. The Axiom of Extensionality implies that $\in$ is set-like.

Exercise 2.1. Let R be a set-like well-founded relation on a class C. Show that every non-empty subclass of C has an R-minimal element.

Hint: This might be harder than it seems at first sight. For a set $S \subseteq C$ define

$$\mathrm{Ext}_R(S) = S \cup \bigcup \{\mathrm{ext}_R(a) : a \in S\}$$

and

$$\mathrm{Ext}_R^\infty(S) = \bigcup \{\mathrm{Ext}_R^n(S) : n \in \mathbb{N}\}.$$

Now, if D is a non-empty subclass of C, pick $a \in D$ and consider the set $D \cap \mathrm{Ext}_R^\infty(\{a\})$. (Why is this a set? You may take recursion on the natural numbers for granted.)

Because of the usefulness of this exercise, whenever we consider a well-founded relation, we will automatically assume that it is set-like.

Theorem 2.2 (Transfinite Induction)**.** *Let C be a class, R a well founded relation on C, $\varphi(x, y_1, \ldots, y_n)$ a formula and $b_1, \ldots, b_n \in C$. If for all $a \in C$ it holds that*

$$\textit{if } \varphi[b, b_1, \ldots, b_n] \textit{ for all } b \in \mathrm{ext}_R(a), \textit{ then } \varphi[a, b_1, \ldots, b_n],$$

then for all $a \in C$, $\varphi[a, b_1, \ldots, b_n]$.

Exercise 2.3. Give a proof of Theorem 2.2.

Theorem 2.4 (Recursion Theorem). *Let C be a class, R a well-founded relation on C and $F : V \to V$ a function. Then there is exactly one function $G : C \to V$ such that for all $a \in C$,*

$$(*) \qquad G(a) = F(a, G \restriction \operatorname{ext}_R(a)).$$

Proof. We first show uniqueness. Let G and G' be functions on C that both satisfy $(*)$ and assume that they are not the same. By Exercise 2.1 there is $a \in C$ which is R-minimal with the property that $G(a) \neq G'(a)$. But now by $(*)$,

$$G(a) = F(a, G \restriction \operatorname{ext}_R(a)) = G'(a),$$

a contradiction.

We now show the existence of G. An *initial segment* of C is a set $S \subseteq C$ such that if aRb and $b \in S$, then $a \in S$. Note that for any $a \in C$, $\operatorname{Ext}_R^\infty(\{a\})$ is an initial segment of C. In fact, $\operatorname{Ext}_R^\infty(\{a\})$ is the smallest initial segment containing a.

Let $\mathcal{G}$ be the collection (class) of all functions g that are defined on an initial segment of C such that for all $a \in \operatorname{dom}(g)$ the equation $(*)$ holds for g. Note that trivially, the empty function is an element of $\mathcal{G}$. By the proof of uniqueness of G, any two functions $g, g' \in \mathcal{G}$ agree on the intersection of their domains, which happens to be an initial segment of C.

It follows that $G = \bigcup \mathcal{G}$ is a function. If $a \in \operatorname{dom}(G)$, then there is $g \in \mathcal{G}$ such that $a \in \operatorname{dom}(g)$. Now $G \restriction \operatorname{ext}_R(a) = g \restriction \operatorname{ext}_R(a)$ and hence G satisfies $(*)$ for all $a \in \operatorname{dom}(G)$. Now assume that $\operatorname{dom}(G) \neq C$. Let a be R-minimal with $a \notin \operatorname{dom}(G)$. Let

$$g = G \restriction \operatorname{Ext}_R^\infty(\operatorname{ext}_R(a)) = G \restriction (\operatorname{Ext}_R^\infty(\{a\}) \setminus \{a\}).$$

We extend g to $g' : \operatorname{Ext}_R^\infty(\{a\}) \to V$ by letting $g'(a) = F(a, g)$. Now $g' \in \mathcal{G}$ and $a \in \operatorname{dom}(g')$. Therefore $a \in \operatorname{dom}(G)$, a contradiction.

Note that if C is a proper class, then so is G. But a class is a collection of sets that is definable by a formula. What is the formula that defines G?

A pair (b, c) of sets is in G iff there is a set g that happens to be a function that is defined on an initial segment of C and satisfies $(*)$ for all a in its domain such that $b \in \operatorname{dom}(g)$ and $g(b) = c$. This is tedious but certainly possible to express in our formal language of set theory. $\square$

2.3. Ordinals, cardinals and arithmetic.

A set a is *transitive* if for all $b \in a$ and all $c \in b$, $c \in a$.

Exercise 2.5. Let a be transitive. Show that $a \cup \{a\}$ and $\mathcal{P}(a)$ are transitive.

Exercise 2.6. Let X be a transitive set. Show that $(X, \in)$ satisfies the Axiom of Extensionality. Find a set X such that $(X, \in)$ does not satisfy the Axiom of Extensionality.

An *ordinal* is a transitive set that is linearly ordered by $\in$. The (proper) class of all ordinals is denoted by Ord. If α and β are ordinals, then $\alpha < \beta$ iff $\alpha \in \beta$. Ord is linearly ordered by $<$, i.e., by $\in$. The Axiom of Foundation implies that $<$ is a well-ordering of Ord. If α is an ordinal, then $\alpha \cup \{\alpha\}$ is the smallest ordinal that is bigger than α. $\alpha \cup \{\alpha\}$ is frequently denoted by $\alpha + 1$, where the $+$ is the $+$ of ordinal arithmetic, not of cardinal arithmetic, which we will discuss below. An ordinal of the form $\alpha + 1$ is a *successor ordinal*. An ordinal different from $0 = \emptyset$ that is not a successor ordinal is a *limit ordinal*.

Two sets a and b are of the same size if there is a bijection between them. A *cardinal* is an ordinal α that is not of the same size as any smaller ordinal. The (proper) class of cardinals is denoted by Card. The *cardinality* of a set a is the

least ordinal that is of the same size as a. It follows from the Axiom of Choice that every set has a cardinality, and the cardinality of a set is always a cardinal. Every infinite cardinal is a limit ordinal.

If κ and λ are cardinals, then $\kappa + \lambda$ is the size of $(\{0\} \times \kappa) \cup (\{1\} \times \lambda)$ and $\kappa \cdot \lambda$ is the size of $\kappa \times \lambda$. κ^λ is the size of the set of all functions from λ to κ.

Theorem 2.7. *If κ and λ are cardinals and at least one of them is infinite, then*

$$\kappa \times \lambda = \kappa + \lambda = \max(\kappa, \lambda).$$

The finite ordinals happen to be cardinals and are denoted by $0, 1, 2, \ldots$. Recall that $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$ and so on. The set of all finite ordinals is ω, the first infinite ordinal. For every ordinal α the α-th infinite cardinal is denoted by $\aleph_\alpha$. In other words, the first infinite cardinals are $\omega = \aleph_0$, $\aleph_1$, $\aleph_2$ and so on.

$\aleph_0$ is the size of the set $\mathbb{N} = \omega$. $2^{\aleph_0}$ is the size of the set $\mathbb{R}$ of real numbers which is the same as the size of $\mathcal{P}(\omega)$.

Theorem 2.8. *For every cardinal κ, $2^\kappa > \kappa$.*

By this theorem, the first candidate for $2^{\aleph_0}$ is $\aleph_1$. The statement $2^{\aleph_0} = \aleph_1$ is known as the *Continuum Hypothesis* (*CH*). The main goal of this course is to show that CH can be neither proved nor refuted from the axioms of ZFC.

Note that Theorem 2.8 implies that for every cardinal there is a larger cardinal. If κ is a cardinal, then the smallest cardinal (strictly) larger than κ is denoted by κ^+. The *Generalized Continuum Hypothesis* (*GCH*) is the statement that for every infinite cardinal κ we have $2^\kappa = \kappa^+$.

Let α be an ordinal. $A \subseteq \alpha$ is *cofinal* (in α) iff for all $\beta < \alpha$ there is $\gamma \in A$ such that $\beta \leq \gamma$. The *cofinality* $\mathrm{cf}(\alpha)$ of an ordinal α is the least size of a cofinal subset of α. A cardinal κ is *regular* if $\kappa = \mathrm{cf}(\kappa)$, otherwise it is *singular*. Cofinalities of ordinals turn out to be regular cardinals.

Exercise 2.9. Show that $\aleph_1$ is regular and $\aleph_\omega$ is singular.

Hint: If A is cofinal in $\aleph_1$, then $\aleph_1 = \bigcup A$. (Why?) If $A \subseteq \aleph_1$ is countable, what is the size of $\bigcup A$? For the singularity of $\aleph_\omega$ use the fact that the union of a set of cardinals, i.e., the supremum of the set of cardinals, is again a cardinal.

The only limitation to the possible values of $2^{\aleph_0}$ is the following strengthening of Theorem 2.8.

Theorem 2.10. *Let κ be an infinite cardinal. Then $\kappa < \mathrm{cf}(2^\kappa)$.*

3. The consistency of the Axiom of Foundation

In this section we show that ZF is consistent provided that ZF without the Axiom of Foundation is consistent. This *relative consistency proof* is technically very easy but nevertheless already uses important ideas that can be used for other consistency proofs as well.

Let ZF^- denote ZF without the Axiom of Foundation.

Theorem 3.1. *If ZF^- is consistent, then so is ZF.*

Proof. Assume that ZF^- is consistent. Then this theory has a model $(V, \in)$. We use $(V, \in)$ in order to construct a model of ZF. To do this, we pretend to live inside V. The ordinals are the ordinals of V, the cardinals are the cardinals of V, and so on. Note that we should adjust our definition of ordinals so that we arrive at the same notion as in the context of Foundation: an ordinal is a transitive set that is well-ordered (rather than just linearly ordered) by $\in$. It can be shown without the Axiom of Foundation that the class Ord of ordinals is well-ordered by $\in$.

For $\alpha \in$ Ord let V_α be defined by

   (i) $V_0 := \emptyset$
   (ii) $V_{\alpha+1} := \mathcal{P}(V_\alpha)$
   (iii) $V_\alpha := \bigcup_{\beta < \alpha} V_\beta$, if α is a limit ordinal.

Using transfinite induction we show that $(V_\alpha)_{\alpha \in \mathrm{Ord}}$ is a strictly $\subseteq$-increasing sequence of transitive sets.

Let WF $= \bigcup_{\alpha \in \mathrm{Ord}} V_\alpha$, i.e., let WF be the class consisting of all sets a such that for some ordinal α, $a \in V_\alpha$. For every $a \in$ WF let rk(a) denote the least ordinal such that $a \in V_{\alpha+1}$. The ordinal rk(a) is the *rank* of a. Note that every ordinal α is an element of WF with rk$(\alpha) = \alpha$.

We show that $(WF, \in)$ is a model of ZF. Set Existence is obviously satisfied. It follows from the transitivity of the V_α that WF is transitive. Hence, WF satisfies the Axiom of Extensionality. The Axiom of Separation follows directly from the construction of the V_α. Namely, if a is an element of V_α, then so is every subset of a. The Axioms of Infinity, Union, and Pairing are easily checked.

For the Axiom of Replacement let F be a function, i.e., a class of pairs in WF such that for all $a \in WF$ there is at most one $b \in WF$ such that $(a, b) \in F$. Now consider the function rk $\circ F$. For every $a \in WF$, $F[a]$ und $(\mathrm{rk} \circ F)[a]$ are sets in V since $(V, \in)$ satisfies Replacement. We have to find a superset of $F[a]$ in WF. It follows from Separation the $F[a]$ is a set in WF. Let $\alpha := \sup((\mathrm{rk} \circ F)[a])$. Now $F[a] \subseteq V_{\alpha+1}$ and $V_{\alpha+1} \in V_{\alpha+2} \subseteq WF$. It follows that $(WF, \in)$ satisfies replacement.

It remains to show that $(WF, \in)$ satisfies the Axiom of Foundation. Let $a \in WF$. Let $b \in a$ be of minimal rank. Then b is an $\in$-minimal element of a since for all $c, d \in WF$ with $c \in d$ we have rk$(c) <$ rk(d). □

While this proof looks convincing at first sight, it does have a couple of problems. First of all, it is a bit confusing to denote a model of ZF^- by $(V, \in)$, since we don't assume $\in$ to be the real $\in$-relation and also the real V is not a set, while structures for the language of set theory are assumed to be sets. On the other hand, for someone living inside the structure, the elements of the structure do form the class of all sets and the binary relation of the structure is simply the $\in$-relation. Looking at the structure from the outside, it should be denoted by $M = (X, E)$ or something similar. This is what we will do from now on.

The class WF of M, really a formula with a single free variable defining the class, has been tacitly identified with the subset of X the consists of all $a \in X$ that

satisfy this formula in the structure M. Then we showed that this subset of X with the restriction of E to it is a model of ZF.

It is possible to completely ingnore the world outside M in the proof of Theorem 3.1. In this case the notation $(V, \in)$ for M is again appropriate. We again define the class WF. But now the statement "WF is a model of ZF" does not make sense anymore, since WF is a class and not a set. Still, it is possible to formalize that $(WF, \in)$ is a model of a certain sentence φ.

Let C be a class and φ a formula. The *relativization* of φ to C is the formula φ^C that is obtained by replacing every quantifier $\exists x$ that occurs in φ by $\exists x \in C$. (Recall that $\forall x$ is just an abbreviation and therefore we do not have to consider this quantifier here.) Of course, here $\exists x \in C \psi$ is just an abbreviation for a more complicated formula that depends on the formula that defines C. Now "$(WF, \in)$ is a model of ZF" can be expressed by saying that for every axiom φ of ZF, φ^{WF} holds (in V).

There is one subtle problem if we want to show φ^{WF} for every axiom φ of ZF. Consider for example the axiom Pairing. It looks like we have to show for all $a, b \in WF$ that $\{a, b\}$ is an element of WF. This is easy since by Pairing in V, $\{a, b\}$ is a set in V as well and it easy to check that in fact, $\{a, b\} \in WF$. Something similar is true for Power Set and Union.

Exercise 3.2. Let $a, b \in WF$. Show that $\{a, b\} \in WF$. Also, show that $\mathcal{P}(a)$ and $\bigcup a$ are elements of WF.

It is, however, not totally obvious that the set that satisfies the definition of $\{a, b\}$ in V also satisfies this definition in WF. Similarly, we have to show that the sets that satisfy the definition of $\bigcup a$ and of $\mathcal{P}(a)$ in V satisfy the same definition in WF. Luckily, these definitions are simple enough that an element of WF satisfies the respective definition in V if and only if it satisfies that definition relativized to WF.

We introduce *absoluteness* in order to deal with this problem explicitly.

Definition 3.3. Let C be a class and $\varphi(x_1, \ldots, x_n)$ a formula. The formula φ is *absolute* over C if the following holds:

$$\forall x_1, \ldots, x_n \in C(\varphi(x_1, \ldots, x_n) \leftrightarrow \varphi^C(x_1, \ldots, x_n))$$

A function (possibly a proper class) is *absolute* over C if the formula that defines it is absolute over C.

Obviously, every formula that does not have any quantifiers (i.e., Boolean combinations of atomic formulas) of is absolute over every class. Quantifiers of the form $\exists x \in y$ are *bounded*. A formula φ is Δ_0 if all quantifiers of φ are bounded.

Lemma 3.4. Δ_0-*formulas are absolute over transitive classes.*

Let C be a class that satisfies a certain fragment ZF^* of ZF, i.e., assume that φ^C holds for every $\varphi \in \text{ZF}^*$. Let φ be a formula and suppose that ZF^* implies that φ is equivalent to a Δ_0-formula. Then φ is absolute over transitive classes that satisfy ZF^*.

It follows that intersections, unions, unordered pairs, ordered pairs, the empty set and so on are absolute over transitive classes that satisfy all the axioms of ZF^- except possibly Power Set and Infinity.

Now suppose that C is a transitive class that satisfies enough of ZF to show the recursion theorem. Then the function $\alpha \mapsto V_\alpha$ is absolute over C in the sense that the formula $\varphi(x, y)$ that says that y is an ordinal α and x is an element of V_α is absolute over C.

From this absoluteness of the V_α it follows that WF is a model of $V = WF$. By transfinite induction over $\in$ it can be shown that assuming ZF^-, $V = WF$ is equivalent to the Axiom of Foundation.

Exercise 3.5. Show that ZF implies that $V = WF$

4. Elementary Submodels, the Reflection Principle, and the Mostowski Collapse

Let (M, E) be a set with a binary relation E. We will often identify M with (M, E). If E is clear from the context, this is not going to lead to confusion. This is actually quite common throughout mathematics: we seldomly distinguish between the field $(\mathbb{R}, 0, 1, +, \cdot)$ of real numbers and the set $\mathbb{R}$.

Now $N \subseteq M$ is an *elementary substructure* or an *elementary submodel* of M if for every formula $\varphi(x_1, \ldots, x_n)$ in the language of set theory and all $a_1, \ldots, a_n$ the following holds:

$$(N, E) \models \varphi(a_1, \ldots, a_n) \Leftrightarrow (M, E) \models \varphi(a_1, \ldots, a_n)$$

Note that if we write (N, E) we really mean $(N, E \cap N^2)$.

The Incompleteness Theorems imply that there cannot be a set N (in V) such that $(N, \in)$ is an elementary submodel of $(V, \in)$. This is Tarski's "undefinability of truth". In other words, there are no sets over which all formulas are absolute. However, we will soon see that for a given finite sets of formulas it is possible to construct even transitive sets such that all of the finitely many formulas under consideration are absolute over the transitive set.

We will use this in the following way: In order to prove the consistency of $\mathrm{ZFC}+\neg\mathrm{CH}$ we pretend that there is a transitive set M such that $(M, \in)$ is a model of ZFC. Using M we construct another transitive set N such that $(N, \in)$ satisfies ZFC but not CH.

Now, if $\mathrm{ZFC}+\neg\mathrm{CH}$ failed to be consistent, then, by the Compactness Theorem, there is already a finite subset of $\mathrm{ZFC}+\neg\mathrm{CH}$ that leads to a contradiction. But in order to prove that these finitely many sentences hold in $(N, \in)$, we only need that $(M, \in)$ satisfies a certain finite subset of ZFC. And for finitely many sentences there are transitive sets M such that these finitely many sentences are absolute over M.

We start with a lemma that will save us some work.

Lemma 4.1. *Let C be a class and $\varphi_1, \ldots, \varphi_n$ a sequence of formulas that is closed under taking subformulas. Recall that only $\exists$ is part of our language, $\forall$ is an abbreviation. Then the formulas $\varphi_1, \ldots, \varphi_n$ are absolute over C if for all $\varphi_i(y_1, \ldots, y_m)$ of the form $\exists x \varphi_j(x, y_1, \ldots, y_n)$ we have*

$$\forall y_1, \ldots, y_m \in C(\exists x \varphi_j(x, y_1, \ldots, y_m) \to \exists x \in C \varphi_j(x, y_1, \ldots, y_m)).$$

Exercise 4.2. Give the proof of Lemma 4.1. Use induction over the length of φ_i.

Theorem 4.3 (Reflection Principle)**.** *Let $W : \mathrm{Ord} \to V$ be a function with the following properties:*

   (i) *For all $\alpha, \beta \in \mathrm{Ord}$ with $\alpha < \beta$ we have $W(\alpha) \subseteq W(\beta)$.*
   (ii) *If γ is a limit ordinal, then $W(\gamma) = \bigcup_{\alpha < \gamma} W(\alpha)$.*
   (iii) *$V = \bigcup_{\alpha \in \mathrm{Ord}} W(\alpha)$.*

For every sequence $\varphi_1, \ldots, \varphi_n$ of formulas and all $\alpha \in \mathrm{Ord}$ there is $\beta \in \mathrm{Ord}$ with $\beta > \alpha$ such that the φ_j are absolute over $W(\beta)$.

Proof. Let $\varphi_1, \ldots, \varphi_n$ be formulas and $\alpha \in \mathrm{Ord}$. We may assume that the sequence $\varphi_1, \ldots, \varphi_n$ is closed under taking subformulas. By Lemma 4.1 it is sufficient to find $\beta > \alpha$ such that for all $\varphi_i(y_1, \ldots, y_{m_i})$ of the form $\exists x \varphi_j(x, y_1, \ldots, y_{m_i})$ we have

$$(*) \quad \forall y_1, \ldots, y_{m_i} \in W(\beta)(\exists x \varphi_j(x, y_1, \ldots, y_{m_i}) \to \exists x \in W(\beta) \varphi_j(x, y_1, \ldots, y_{m_i})).$$

For every $i \in \{1, \ldots, n\}$ we define a function G_i as follows: Suppose $\varphi_i(y_1, \ldots, y_{m_i})$ is of the form $\exists x \varphi_j(x, y_1, \ldots, y_{m_i})$. Let $G_i(b_1, \ldots, b_{m_i}) = 0$ if there is no a such that $\varphi_j(a, b_1, \ldots, b_{m_i})$ holds in V. If there is a such that $\varphi_j(a, b_1, \ldots, b_{m_i})$ holds in V, then let $G_i(b_1, \ldots, b_{m_i})$ be the least ordinal α such that there is such an a in $W(\alpha)$. Note that the existence of α follows from (iii).

Now we choose a sequence $(\beta_k)_{k \in \omega}$ as follows: Let $\beta_0 = \alpha$. Suppose we have defined β_k for some $k \in \omega$. Let β_{k+1} be the least ordinal $> \beta_k$ such that for all $\varphi_i(y_1, \ldots, y_{m_i})$ and all $b_1, \ldots, b_{m_i}$ in $W(\beta_k)$, $G_i(b_1, \ldots, b_{m_i}) < \beta_{k+1}$.

Let $\beta = \sup_{k \in \omega} \beta_k$. Now it is easily checked that for each $\varphi_i(y_1, \ldots, y_{m_i})$ and all $b_1, \ldots, b_{m_i} \in W(\beta)$, $G_i(b_1, \ldots, b_{m_i}) < \beta$. Hence, by the choice of the G_i and by Lemma 4.1, all the φ_i are absolute over $W(\beta)$. □

Observe that the function $\alpha \mapsto V_\alpha$ satisfies all the assumptions of Theorem 4.3. In particular, if V satisfies ZFC, then for every finite list $\varphi_1, \ldots, \varphi_n$ of axiom in ZFC there are arbitrarily large α such that $(V_\alpha, \in)$ satisfies $\varphi_1, \ldots, \varphi_n$.

A proof very similar to the proof of Theorem 4.3 yields

Theorem 4.4 (Löwenheim-Skolem Theorem, downward). *Let (M, E) be a structure for the language of set theory. For every $X \subseteq M$ there is an elementary submodel $N \subseteq M$ of M such that $X \subseteq N$ and $|N| \leq |X| + \aleph_0$.*

Proof. As in the proof of Theorem 4.3 it is enough to find $N \subseteq M$ with $X \subseteq N$ and $|N| = |X| + \aleph_0$ such that for every existential formula $\varphi(x, y_1, \ldots, y_n)$ and all $b_1, \ldots, b_n \in N$ with

$$M \models \exists x \varphi(b_1, \ldots, b_n)$$

there is $a \in N$ such that

$$M \models \varphi(a, b_1, \ldots, b_n).$$

For every formula $\varphi(x, y_1, \ldots, y_n)$ we define a function $f_\varphi : M^n \to M$ such that for all $b_1, \ldots, b_n \in M$ we have

$$M \models \varphi(f_\varphi(b_1, \ldots, b_n), b_1, \ldots, b_n)$$

provided

$$M \models \exists x \varphi(b_1, \ldots, b_n).$$

The f_φ are called *Skolem functions*.

For every $X \subseteq M$ let $\mathrm{sk}(X)$ be the *Skolem hull* of X, i.e., the closure of X under all the functions f_φ. Since there are only countably many formulas and hence only countably many Skolem functions, for every $X \subseteq M$, $|\mathrm{sk}(X)| \leq |X| + \aleph_0$. Clearly, $N = \mathrm{sk}(X)$ satisfies all existential statements with parameters in N that are satisfied in M. Hence, N is an elementary submodel of M. □

Now, if V satisfies all axioms of ZFC, we can carry out the following construction. Let Σ be a finite collection of axioms of ZFC. By the Reflection Principle there is α such that all $\varphi \in \Sigma$ are absolute over V_α. Since $(V, \in)$ satisfies Σ, $(V_\alpha, \in)$ is a model of Σ as well. By the Löwenheim-Skolem Theorem, V_α has a countable elementary submodel N. This shows that every finite collection of axioms of ZFC has a countable model (assuming that V satisfies ZFC). We will proceed by constructing countable transitive models of finite parts of ZFC.

Theorem 4.5 (Mostowski Collapse). *Let C be a class and R a well-founded relation on C (recall that we assume well-founded relations to be set-like). If R is extensional, i.e., if two elements a and b of C agree iff $\mathrm{ext}_R(a) = \mathrm{ext}_R(b)$, then there are a transitive class D and an isomorphism $\mu : (C, R) \to (D, \in)$.*

Proof. We define μ by recursion on R. For every $a \in C$ let

$$\mu(a) = \{\mu(b) : b \in \text{ext}_R(a)\}.$$

By the Recursion Theorem, μ is a well-defined function from C to V. Let $D = \{\mu(a) : a \in C\}$. The function μ is the *Mostowski collapsing function* and D is the *Mostowski collapse* of (C, R).

We first show that μ is 1-1. Suppose it is not and let $a \in C$ be R-minimal such that for some $b \in C$ we have $a \neq b$ and $\mu(a) = \mu(b)$. By the definition of μ, $\mu(a) = \{\mu(c) : c \in \text{ext}_R(a)\}$. Since $\mu(a) = \mu(b)$,

$$\{\mu(c) : c \in \text{ext}_R(a)\} = \{\mu(c) : c \in \text{ext}_R(b)\}.$$

But since a is an R-minimal counter-example to the injectivity of μ, we can conclude that $\text{ext}_R(a) = \text{ext}_R(b)$. Now the extensionality of R implies $a = b$, a contradiction.

Clearly, if $a, b \in C$ are such that aRb, then $\mu(a) \in \mu(b)$. On the other hand, if $\mu(a) \in \mu(b)$, then, since μ is 1-1, $a \in \text{ext}_R(b)$, i.e., aRb. This shows that μ is an isomorphism.

It remains to show that D is a transitive class. Let $a \in D$ and $b \in a$. Choose $c \in C$ such that $a = \mu(c)$. By the definition of μ, b is of the form $\mu(d)$ for some $d \in \text{ext}_R(c)$. But then $d \in C$ and thus $b = \mu(d) \in D$. $\qquad\square$

Our main application of the Mostowski Collapse is

Corollary 4.6. *Every finite fragment of ZFC has a countable transitive model.*

Proof. Let Σ be a finite fragment of ZFC. We may assume that Σ contains the Axiom of Extensionality. We have already argued that Σ has a countable model of the form $(N, \in)$. Since N satisfies the Axiom of Extensionality, $\in$ is extensional on N. Therefore $(N, \in)$ is isomorphic to a structure $(M, \in)$ where M is transitive. But since $(N, \in)$ and $(M, \in)$ are isomorphic, they satisfy the same sentences. Clearly, M is countable. $\qquad\square$

Exercise 4.7. Let C be a class on which $\in$ is extensional. Suppose T is a transitive (in V) subclass of C. Let D be the Mostowski collapse of $(C, \in)$ and let μ be the collapsing function. Show that μ is the identity on T. In particular, $T \subseteq D$.

5. Constructibiltiy

In ZF we will define a class L that satisfies ZFC+GCH. Recall that GCH is the statement

$$\forall \kappa \in \mathrm{Card}(\kappa \geq \aleph_0 \to 2^\kappa = \kappa^+).$$

L is Gödel's universe of *constructible sets*. Since we want to show the consistency of the Axiom of Choice (AC) with ZF, we have to be careful not to use AC in the following arguments. We will explicit indicate uses of AC in certain places that are not essential for the theory.

5.1. **Definability.**
The construction of L will be very similar to the construction of WF in that we define a hierarchy $(L_\alpha)_{\alpha \in \mathrm{Ord}}$ using some restricted power set operation.

First of all we recall that formulas can be regarded as certain sets, namely finite sequences of elements from our alphabet where the alphabet consists of sets. I.e., we code the characters of the alphabet by certain sets, say "(" by 0, ")" by 1, "="by 2 and so on.

For a finite sequence φ of characters in the real world let $\ulcorner \varphi \urcorner$ denote its character-by-character translation into the finite sequence (a set) of sets that we used to code the respective characters. $\ulcorner \varphi \urcorner$ is the *Gödelization* of φ. Using the Recursion Theorem we can now write down a formula $\mathrm{fml}(x)$ in the real world that expresses the fact that x is a finite sequence of characters from our alphabet that happens to be a formula in the language of set theory. We can then prove for every formula φ in the real world that $\ulcorner \varphi \urcorner$ actually satisfies fml.

Again using the Recursion Theorem we can write down a formula (in the real world) $\mathrm{sat}(x, y, z)$ that says:

(i) There is $n \in \omega$ such that y is a formula with n free variables,
(ii) there are $a_1, \ldots, a_n \in x$ such that $z = (a_1, \ldots, a_n)$ and
(iii) the structure $(x, \in)$ satisfies the formula y if the free variables of y are interpreted by $a_1, \ldots, a_n$.

By induction over the complexity of formulas we can show that for every formula $\varphi(x_1, \ldots, x_n)$, every set M and all $a_1, \ldots, a_n \in M$ it holds that

$$\varphi^M(a_1, \ldots, a_n) \leftrightarrow \mathrm{sat}(M, \ulcorner \varphi \urcorner, (a_1, \ldots, a_n))$$

Hence the relation $\models$ can now be regarded as a definable class (where we consider $\models$ only for structures of the form $(M, \in)$, but the general case (M, E) can be handled practically in the same way).

Note that in the definition of the formula sat we used the fact that we can code the finitely many sets $a_1, \ldots, a_n$ into a single set, namely the n-tuple $(a_1, \ldots, a_n)$. This is necessary since the formula sat has to have a fixed number of free variables.

We can easily write down a formula that defines the set ZFC of formulas. We can then prove that every sentence in the real-world ZFC has its Gödelization in V's version of ZFC. If we are a little bit more general in the definition of sat, so that sat applies to structures of the form (M, E), we can write down the formula $\mathrm{Con}(x)$ that says that x is a set of sentences that has a model. Gödel's Second Incompleteness Theorem now states that $\mathrm{Con}(\mathrm{ZFC})$ is not provable from ZFC. Note that the first ZFC is the set satisfying the definition of ZFC in V where the second ZFC is the real-world (meta-mathematical) ZFC.

Now let M be a set. A set $P \subseteq M$ is *definable* (in $(M, \in)$) if there is a formula $\varphi(x, y_1, \ldots, y_n)$ such that for some parameters $b_1, \ldots b_n \in M$ we have

$$P = \{a \in M : (M, \in) \models \varphi(a, b_1, \ldots, b_n)\}.$$

Using the formula sat we can define a function $\mathcal{D}$ that assigns to each set M the set $\mathcal{D}(M)$ of subsets of M that are definable in $(M, \in)$. For every set M and every real-world formula $\varphi(x, y_1, \ldots, y_n)$ we can show that for all $b_1, \ldots, b_n \in M$ we have

$$\{a \in M : \varphi^M(a, b_1, \ldots, b_n)\} \in \mathcal{D}(M).$$

Lemma 5.1. *Let M be a set. Then the following hold:*

(1) $\mathcal{D}(M) \subseteq \mathcal{P}(M)$
(2) *If M is transitive, then $\mathcal{D}(M)$ and $M \subseteq \mathcal{D}(M)$.*
(3) $\forall X \subseteq M(|X| < \omega \rightarrow X \in \mathcal{D}(M))$
(4) *(AC)* $|M| \geq \omega \rightarrow |\mathcal{D}(M)| = |M|$

Proof. (1) is obvious. For (2) let M be transitive and $a \in M$. Then $a = \{x \in M : x \in a\}$. Hence a is a definable subset of M and thus $a \in \mathcal{D}(M)$. Since a was arbitrary, this shows $M \subseteq \mathcal{D}(M)$. Now let $a \in \mathcal{D}(M)$ and let $b \in a$. Since $a \subseteq M$, $b \in M$. But since $M \subseteq \mathcal{D}(M)$, $b \in \mathcal{D}(M)$. This shows that $\mathcal{D}(M)$ is transitive.

(3) In V we use induction over the size of X. Clearly, the empty set is definable. Now let $n \in \omega$ and let $f : n+1 \rightarrow X$ be a bijection. By our inductive hypothesis, $f[n]$ is a definable subset of M, for instance $f[n] = \{x \in M : M \models \varphi(x, b_1, \ldots, b_m)\}$ for some $b_1, \ldots, b_m \in M$. Now

$$f[n+1] = \{x \in M : M \models \varphi(x, b_1, \ldots, b_m) \vee x = b_{m+1}\},$$

where we choose $b_{m+1} = f(n)$.

(4) easily follows from the facts that the language of set theory has only countably many formulas and that for every $n \in \omega$ there are only $|M|$ n-tuples of parameters from M. $\square$

5.2. **The definition of L and its elementary properties.**

Definition 5.2. For each ordinal α we define L_α recursively as follows:

(i) $L_0 := \emptyset$
(ii) $L_{\alpha+1} := \mathcal{D}(L_\alpha)$
(iii) $L_\alpha := \bigcup_{\beta < \alpha} L_\beta$ if α is a limit ordinal.

Let $L := \bigcup_{\alpha \in \text{Ord}} L_\alpha$ be the class of *constructible sets*.

Using Lemma 5.1 by transfinite induction we easily get

Lemma 5.3. *For all $\alpha \in \text{Ord}$ the set L_α is transitive. For all $\alpha, \beta \in \text{Ord}$ with $\alpha \leq \beta$ we have $L_\alpha \subseteq L_\beta$.*

In particular, the Reflection Principle relativized to L applies to the function $\alpha \mapsto L_\alpha$.

Definition 5.4. For every $a \in L$ we define the *L-rank* $\rho(a)$ of a to be the least $\alpha \in \text{Ord}$ such that $a \in L_{\alpha+1}$.

Lemma 5.5. *For all $\alpha \in \text{Ord}$ we have the following:*

(1) $L_\alpha = \{a \in L : \rho(a) < \alpha\}$
(2) $L_\alpha \cap \text{Ord} = \alpha$
(3) $\alpha \in L$ and $\rho(\alpha) = \alpha$
(4) $L_\alpha \in L_{\alpha+1}$
(5) *Every finite subset of L_α is an element of $L_{\alpha+1}$.*

Proof. (1) is immediate from the definition of ρ. We show (2) by induction on α. If $\alpha = 0$, then $L_\alpha = \emptyset = 0 \cap \text{Ord}$. If α is a limit ordinal, then

$$\alpha = \bigcup_{\beta < \alpha} \beta = \bigcup_{\beta < \alpha} L_\beta \cap \text{Ord} = L_\alpha \cap \text{Ord} \,.$$

Now let $\alpha = \beta + 1$. Then $\beta = L_\beta \cap \text{Ord}$. But the definition of the class of ordinals is Δ_0 and hence absolute over the transitive class L_β. Thus, β is a definable subset of L_β, namely $\beta = \{a \in L_\beta : (L_\beta, \in) \models a \text{ is an ordinal}\}$. Hence $\beta \in L_{\beta+1}$. On the other hand, α is not a subset of L_β, simply because $\beta \notin L_\beta$. The same holds for every ordinal $\geq \alpha$. Hence $\alpha = L_\alpha \cap \text{Ord}$.

(3) follows immediately from (2). (4) is obvious. $\qquad\square$

Lemma 5.6. *a) For all $\alpha \in \text{Ord}$ we have $L_\alpha \subseteq V_\alpha$.*
b) For all $n \in \omega$, $L_n = V_n$. Moreover, $L_\omega = V_\omega$.
c) Assuming AC, for all $\alpha \geq \omega$, $|L_\alpha| = |\alpha|$.

Proof. a) follows from the fact that $\mathcal{D}(M) \subseteq \mathcal{P}(M)$ for all sets M.

Since all finite subsets of a set are definable, for every finite set M we have $\mathcal{D}(M) = \mathcal{P}(M)$. This implies $L_n = V_n$ for every finite ordinal n. Now $L_\omega = \bigcup_{n \in \omega} L_n = \bigcup_{n \in \omega} V_n = V_\omega$. This shows b).

For c) observe that since all the L_n are finite, $|L_\omega| = \aleph_0$. Now, since for every infinite set M we have $|\mathcal{D}(M)| = |\mathcal{M}|$ transfinite induction on α shows $|L_\alpha| = |\alpha|$ for all $\alpha \geq \omega$. $\qquad\square$

5.3. ZF in L. We assume that V satisfies ZF and show that L satisfies ZF as well. That AC and GCH are satisfied in L requires some more work.

Theorem 5.7. *L satisfies ZF.*

Proof. Being an increasing union of transitive sets, the class L itself is transitive. Hence it satisfies the Axiom of Extensionality. Clearly, $\emptyset \in L$ and hence Set Existence is satisfied. Foundation holds in L because it holds in V. L satsifies Infinity since $\omega \in L$.

We now show Separation in L. Let $\varphi(x, y_1, \ldots, y_n)$ be a formula and let $a, b_1, \ldots, b_n \in L$. We have to show that $\{x \in a : \varphi^L(x, b_1, \ldots, b_n)\} \in L$. Choose $\alpha \in \text{Ord}$ such that $a, b_1, \ldots, b_n \in L_\alpha$. By the Reflection Principle there is $\beta > \alpha$ such that φ is absolute between L_β and L. Now

$$\{x \in a : \varphi^L(x, b_1, \ldots, b_n)\} = \{x \in a : \varphi^{L_\beta}(x, b_1, \ldots, b_n)\}.$$

Clearly, $\{x \in a : \varphi^{L_\beta}(x, b_1, \ldots, b_n)\} \in \mathcal{D}(L_\beta) = L_{\beta+1} \subseteq L$.

Since the Separation Axiom holds in L, in order to prove Pairing, Union, Power Set and Replacement in L we only have to prove the existence of sufficiently large sets. Good candidates are the L_α. We give the proof of the Power Set Axiom. The proofs of the other axioms are similar but rather easier.

Let $a \in L$ and let $\alpha := \sup\{\rho(b) : b \in L \wedge b \subseteq a\} + 1$. Now for all $b \in L$ with $b \subseteq a$ we have $b \in L_\alpha \in L$. Now the collection of all elements of L that are subsets of a can be obtained from L_α using Separation. $\qquad\square$

5.4. $V = L$? It is a natural question whether V can be the same as L, i.e., whether ZF$+V = L$ is consistent. Intuitively, one would think that L satisfies $V = L$. While this is true, it is an non-trivial fact. It could happen that, when we repeat the construction of L inside L itself, we end up with some class L^L which is a proper subclass of L. Fortunately, this is not the case.

Theorem 5.8. *L satisfies $V = L$.*

Proof. We already know that L contains all the ordinals. Hence, in order to show $(V = L)^L$, it suffices to show that for all $\alpha \in \text{Ord}$ we have $L_\alpha = L_\alpha^L$. Clearly $L_0 = \emptyset = L_0^L$ and the limit stages of this inductive proof are easy.

Now let $\alpha \in \text{Ord}$ and assume $L_\alpha = L_\alpha^L$. Now $L_{\alpha+1} = L_{\alpha+1}^L$ is equivalent to $\mathcal{D}(L_\alpha) = \mathcal{D}^L(L_\alpha)$. The definition of $\mathcal{D}$ is a formula that uses the parameter ω, respectively $\omega^{<\omega} = \bigcup_{n \in \omega} \omega^n$, because that is the set that we use to code formulas as sets. Moreover, the definition of $\mathcal{D}$ uses recursion over ω, but the individual steps in the recursion only use Δ_0-formulas.

It is easily checked that recursively defined functions in which the definitions of the individual steps of the recursion are absolute are again absolute over models of sufficiently large fragments of ZF. This shows that $\mathcal{D}$ is absolute over transitive classes that satisfies ZF without Power Set. (We need some fragment of ZF that allows us to prove the recursion theorem. ZF without Power Set is convenient, works for our purposes and is satisfied by many sets.)

This shows that L and V agree on whether a subset of L_α is definable or not. Hence $\mathcal{D}(L_\alpha) = \mathcal{D}^L(L_\alpha)$. This finishes the proof of the theorem. $\square$

These absoluteness considerations show this: If M is a transitive class that contains all the ordinals and satisfies ZF, then $L \subseteq M$ and $L = L^M$. In other words, L is the smallest transitive class that contains all the ordinals and satisfies ZF.

We will see later that ZF is consistent with $V \neq L$.

5.5. **AC and GCH in L.**

Theorem 5.9. $V = L$ *implies the Axiom of Choice*

The proof of this theorem uses

Lemma 5.10. *Let $\sqsubset$ be a well ordering of a set X.*

a) For all $a_1, \ldots, a_n, b_1, \ldots, b_n \in X$ let $\bar{a} = (a_1, \ldots, a_n) \sqsubset^n \bar{b} = (b_1, \ldots, b_n)$ iff $\bar{a} \neq \bar{b}$ and for the minimal i with $a_i \neq b_i$ it holds that $a_i \sqsubset b_i$. Then $\sqsubset^n$ is a well-ordering on X^n.

b) For all $\bar{a}, \bar{b} \in X^{<\omega} = \bigcup_{n \in \omega} X^n$ let $\bar{a} \sqsubset^{<\omega} \bar{b}$ if either $\bar{a}$ is a shorter finite sequence than $\bar{b}$ or for some $n \in \omega$, $\bar{a}, \bar{b} \in X^n$ and $\bar{a} \sqsubset^n \bar{b}$. Then $\sqsubset^{<\omega}$ is a well-ordering of $X^{<\omega}$.

Exercise 5.11. Prove Lemma 5.10.

Proof of Theorem 5.9. We show a statement stronger than AC. We show that $V = L$ implies that there is a definable binary relation $\lhd$ that is a well-ordering of L. This clearly implies that every constructible set X can be well-ordered, namely by the restriction of $\lhd$ to X.

Recursively, for all $\alpha \in \mathrm{Ord}$ we define well-orderings $\lhd_\alpha$ of L_α such that for $\alpha < \beta$, $(L_\alpha, \lhd_\alpha)$ is an initial segment of $(L_\beta, \lhd_\beta)$, i.e., $\lhd_\alpha = \lhd_\beta \restriction L_\alpha$ and for all $a \in L_\alpha$ and $b \in L_\beta$ with $b \lhd_\beta a$ we have $b \in L_\alpha$.

Obviously, we have to put $\lhd_0 = \emptyset$. If α is a limit ordinal, let $\lhd_\alpha = \bigcup_{\beta < \alpha} \lhd_\beta$. Similarly, let $\lhd = \bigcup_{\alpha \in \mathrm{Ord}} \lhd_\alpha$. The only difficult step is the definition of $\lhd_\alpha$ if $\alpha = \beta + 1$ for some ordinal β.

Assume $\lhd_\beta$ is a wellordering of L_β. Since there are only countably many formulas in the language of set theory, the set of all formulas can be well-ordered. Let $\prec$ be a well-ordering of the set of formulas.

Now let $a, b \in L_\alpha = L_{\beta+1}$. If $a, b \in L_\beta$, let $a \lhd_\alpha b$ iff $a \lhd_\beta b$. If $a \in L_\beta$ and $b \in L_\alpha \setminus L_\beta$, let $a \lhd b$. If $a, b \in L_\alpha \setminus L_\beta$, let $\varphi_a(x_1, \ldots, x_n)$ and $\varphi_b(y_1, \ldots, y_m)$ be $\prec$-minimal formulas defining a, respectively b in $(L_\beta, \in)$ with suitable parameters. Let $(a_1, \ldots, a_n) \in L_\beta^n$ be $\lhd_\beta^n$-minimal with

$$a = \{c \in L_\beta : (L_\beta, \in) \models \varphi_a[c, a_1, \ldots, a_n]\}$$

and let $(b_1, \ldots, b_m) \in L_\beta^m$ be $\lhd_\beta^m$-minimal with

$$b = \{c \in L_\beta : (L_\beta, \in) \models \varphi_b[c, b_1, \ldots, b_m]\}.$$

Now let $a \lhd_\alpha b$ iff either $\varphi_a \prec \varphi_b$ or $\varphi_a = \varphi_b$ and $(a_1, \ldots, a_n) \lhd_\beta^{<\omega} (b_1, \ldots, b_m)$.

This finishes the definition of the $\lhd_\alpha$ and hence of $\lhd$. It is straight forward to verify that the construction works (using the proof of Lemma 5.10). $\square$

In order to show that GCH holds in L we need

Lemma 5.12. *Let $\kappa > \aleph_0$ be a regular cardinal. Then L_κ is a model of ZF without the Power Set Axiom.*

Proof. Since κ is an infinite cardinal, κ is a limit ordinal. The proofs of Set Existence, Extensionality, Pairing and Union in L actually go through for all L_α with α a limit ordinal. In order to show the Separation Scheme, we have to use some form of the Reflection Principle for L_κ.

Let if $\alpha < \kappa$. For each existential formula $\exists x \varphi(x, y_1, \ldots, y_n)$ and all parameters $b_1, \ldots, b_n \in L_\alpha$ with

$$L_\kappa \models \exists x \varphi[b_1, \ldots, b_n]$$

choose $\gamma < \kappa$ such that L_γ already contains a witness to this existential statement. To avoid trivialities, we choose $\gamma > \alpha$.

Let B be the set of all γ's chosen in this way. Since there are only countably many formulas and since L_α is of size $< \kappa$, B is of size $< \kappa$. Since κ is regular, $\beta_0 = \sup(B) < \kappa$. We now replace L_α by L_{β_0} and go through the same process, obtaining $\beta_1 < \kappa$ and so on.

Finally, let $\beta = \sup_{n \in \omega} \beta_n$. Again by the regularity of κ, $\beta < \kappa$. Clearly, L_β is an elementary submodel of L_κ.

We are now ready to show that the Separation Scheme holds in L_κ. Let $\varphi(x, y_1, \ldots, y_n)$ be a formula and $a, b_1, \ldots, b_n \in L_\kappa$. We have to show that

$$d = \{c \in a : L_\kappa \models \varphi[c, b_1, \ldots, b_n]\} \in L_\kappa.$$

Let $\alpha < \kappa$ be such that $a, b_1, \ldots, b_n \in L_\alpha$. By the argument above, there is $\beta < \kappa$ such that $\alpha < \beta$ and L_β is an elementary submodel of L_κ. Now $d = \{c \in a : L_\beta \models \varphi[c, b_1, \ldots, b_n]\}$ is a definable subset of L_β and hence $d \in L_{\beta+1} \subseteq L_\kappa$. This shows Separation.

The proof of Replacement is very similar to the proof of Replacement in L and uses again the regularity of κ and the fact that all elements of L_κ are of size $< \kappa$. $\square$

Theorem 5.13. *$V = L$ implies GCH.*

Proof. Assume $V = L$ and let κ be an infinite cardinal. We show that $\mathcal{P}(\kappa) \subseteq L_{\kappa^+}$ and therefore $2^\kappa \leq \kappa^+$.

Let $a \subseteq \kappa$. By $V = L$ there is a regular cardinal $\lambda > \aleph_0$ such that $a \in L_\lambda$. By the Löwenheim-Skolem Theorem, there is an elementary submodel M of L_λ such that $|M| = \kappa$ and $\kappa \cup \{a\} \subseteq M$. Let N be the transitive collapse of M. Since $a \subseteq \kappa \subseteq \kappa$ and κ is transitive, $\kappa \cup \{a\}$ is transitive. Since Mostowski collapsing functions are the identity on transitive classes, $a \in N$.

Since N is isomorphic to an elementary submodel of L_λ, $N \models V = L$. Since N is a transitive model of ZF without the Power Set Axiom, the absoluteness properties of L give that $N = \bigcup_{\alpha \in N \cap \mathrm{Ord}} L_\alpha = L_\beta$ where $\beta = \sup(N \cap \mathrm{Ord})$. Since M and therefore N are of size κ, $|\beta| = |L_\beta| = \kappa$. In particular, $\beta < \kappa^+$.

It follows that $a \in L_{\kappa^+}$, finishing the proof of the theorem. $\square$

Corollary 5.14. *If ZF is consistent, then so is ZFC+GCH.*

Exercise 5.15. Assume $V = L$. Given an infinite $\alpha < \aleph_1$, give an explicit example of a subset a of ω such that $a \in L_{\aleph_1} \setminus L_\alpha$.

Hint: This actually requires some thought. First of all observe that if $\alpha < \aleph_1$ is large enough, then L_α contains a bijection between ω and $\omega \times \omega$. Using this bijection, relations on ω, i.e., subsets of $\omega \times \omega$, can be coded by subsets of ω. Now, if R is a well-ordering on ω and $\alpha < \aleph_1$ is suitably chosen (say, for example, L_α is an elementary submodel of $L_{\aleph_1}$), then L_α will also contain the unique ordinal that is isomorphic to (ω, R), because we can perform the Mostowski collaps of (ω, R)

inside L_α. What is an example of a set (not necessarily a subset of ω) that is in $L_{\aleph_1}$, but not in L_α?

6. Forcing

In this section we will find a way to enlarge the universe of all sets.

6.1. **Partial orderings, dense sets and filters.**

Definition 6.1. Let $\mathbb{P}$ be a set and $\leq$ a binary relation on $\mathbb{P}$. Then $(\mathbb{P}, \leq)$ is a *partial ordering* or a *partial order* if the following hold:

(i) (Transitivity) $\forall x, y, z \in \mathbb{P}(x \leq y \wedge y \leq z \to x \leq z)$
(ii) (Reflexivity) $\forall x \in \mathbb{P}(x \leq x)$
(iii) (Antisymmetry) $\forall x, y \in \mathbb{P}(x \leq y \wedge y \leq x \to x = y))$

The elements of $\mathbb{P}$ are *conditions*. If $p, q \in \mathbb{P}$ and $p \leq q$ we say that p is *stronger* than q, respectively, p *extends* q. Two conditions p and q are *compatible* if they have a common extension $r \in \mathbb{P}$, i.e., if there is $r \in \mathbb{P}$ such that $r \leq p$ and $r \leq q$. If p and q are not compatible, they are *incompatible* and we write $p \perp q$. For technical reasons we will only consider partial orders $\mathbb{P}$ with a largest element, denoted by 1 or $1_{\mathbb{P}}$. Similarly, when dealing with several partial orders at the same time, we might denote the relation $\leq$ on $\mathbb{P}$ by $\leq_{\mathbb{P}}$. In this case we might also write $\perp_{\mathbb{P}}$ instead of just $\perp$.

Let us consider a couple of examples. $(\mathbb{N}, \leq)$ is not a partial order in our sense, because it does not have a largest element (but of course, it is a perfectly nice partial order in other contexts). $(\mathbb{N}, \geq)$ is a partial order in our sense, but boring, because any two elements are compatible.

Let $\mathbb{O}$ be the collection of all non-empty open subsets of $\mathbb{R}$. $(\mathbb{O}, \subseteq)$ is a very nice partial order in our sense. Two condition $U, V \in \mathbb{O}$ are compatible iff $U \cap V \neq \emptyset$. Clearly, $1_{\mathbb{O}} = \mathbb{R}$.

Let $\mathbb{M}$ denote the collection of all measurable subsets of $\mathbb{R}$ of positive measure. Then $(\mathbb{M}, \subseteq)$ is another nice partial order. $A, B \in \mathbb{M}$ are compatible iff $A \cap B$ is not of measure zero.

Observe that $\mathbb{O}$ and $\mathbb{M}$ are not standard names for these partial orders. Typically one considers closely related Boolean algebras that are, for our purposes, equivalent to $\mathbb{O}$ and $\mathbb{M}$, namely the Cohen-algebra $\mathbb{C}$ and the measure algebra $\mathbb{B}$. We will see later what the connection between partial orders and Boolean algebras is.

Another important family of partial orders arises as follows: Let X be a set. Consider

$$\mathrm{Fn}(X, 2) := \{p : p \text{ is a function from a finite subset of } X \text{ to } 2\}.$$

$\mathrm{Fn}(X, 2)$ is partially ordered by the *reverse inclusion* $\supseteq$. The largest element of $\mathrm{Fn}(X, 2)$ is the empty function. Two conditions $p, q \in \mathrm{Fn}(X, 2)$ are compatible iff $p \cup q$ is a function. The elements of $\mathrm{Fn}(X, 2)$ should be considered as finite approximations of a function from X to 2.

For our purposes, $\mathrm{Fn}(\omega, 2)$ is equivalent to $\mathbb{O}$ and to $\mathbb{C}$. We will later see why this is.

Definition 6.2. Let $(\mathbb{P}, \leq)$ be a partial order. Then $D \subseteq \mathbb{P}$ is *dense* in $\mathbb{P}$ if for all $p \in \mathbb{P}$ there is $q \in D$ such that $q \leq p$. For $p \in \mathbb{P}$ we say that $D \subseteq \mathbb{P}$ is *dense below* p if for all $q \leq p$ there is $r \in D$ such that $r \leq q$. A set $A \subseteq \mathbb{P}$ is an *antichain* if no two distinct elements of A are compatible. A set $G \subseteq \mathbb{P}$ is a *filter* if the following hold:

(i) $\forall p \in \mathbb{P} \forall q \in G(q \leq p \to p \in G)$
(ii) $\forall p, q \in G \exists r \in G(r \leq p \wedge r \leq q)$

If $\mathcal{D}$ is a family of dense subsets of $\mathbb{P}$ and $G \subseteq \mathbb{P}$ a filter, then G is $\mathcal{D}$-generic iff for all $D \in \mathcal{D}$, $G \cap D \neq \emptyset$.

What do dense subsets of $\mathbb{O}$ look like? If $D \subseteq \mathbb{O}$ is any set, then $X = \bigcup D$ is a union of open sets and therefore open. If D is dense, then for every non-empty open set $U \subseteq \mathbb{R}$ there is $V \in D$ such that $V \subseteq U$. In particular, $X \cap U \neq \emptyset$. It follows that X is dense in $\mathbb{R}$ in the topological sense.

On the other hand, if $X \subseteq \mathbb{R}$ is dense and open, consider $D = \{U \subseteq \mathbb{R} : U \subseteq X \text{ is open}\}$. Now for every $V \in \mathbb{O}$, $X \cap V$ is non-empty and open and thus $U = X \cap V \in D$. It follows that D is dense in $\mathbb{O}$ in the order-theoretic sense.

Note however that not every dense subset of $\mathbb{O}$ is the collection of all non-empty open subsets of a dense open set $X \subseteq \mathbb{R}$. An example is the set of all open intervals with rational endpoints. Another example is for $\varepsilon > 0$ the set D_ε of all open intervals of length $< \varepsilon$.

Now let x be a real number and consider $G_x := \{U \in \mathbb{O} : x \in U\}$. It is easily checked that G_x is a filter in $\mathbb{O}$. Moreover, G_x is $(D_\varepsilon)_{\varepsilon>0}$-generic. On the other hand, if $G \subseteq \mathbb{O}$ is a $(D_\varepsilon)_{\varepsilon>0}$-generic filter, then there is exactly one real number x such that $x \in \bigcap_{U \in G} \operatorname{cl}(U)$. Note, however, that $x \in \bigcap G$ can fail.

Exercise 6.3. Consider the partial order $\operatorname{Fn}(\omega, 2)$. Show:
(1) If $G \subseteq \operatorname{Fn}(\omega, 2)$ is a filter, then $\bigcup G$ is a function.
(2) For all $n \in \omega$ the set $D_n := \{p \in \operatorname{Fn}(\omega, 2) : n \in \operatorname{dom}(p)\}$ is dense $\operatorname{Fn}(\omega, 2)$.
(3) If $G \subseteq \operatorname{Fn}(\omega, 2)$ is a $\{D_n : n \in \omega\}$-generic filter, then $\bigcup G$ is a function from ω to 2.
(4) For every function $f : \omega \to 2$ the set $G_f := \{p \in \operatorname{Fn}(\omega, 2) : p \subseteq f\}$ is a $\{D_n : n \in \omega\}$-generic filter.

The next theorem is a version of the Baire Category Theorem and guarantees the existence of sufficiently generic filters.

Theorem 6.4. *(Rasiowa-Sikorsky) Let $(\mathbb{P}, \leq)$ be a partial order and let $\mathcal{D}$ be a countable family of dense subsets of $\mathbb{P}$. Then there is a $\mathcal{D}$ generic filter $G \subseteq \mathbb{P}$.*

Proof. Let $\{D_n : n \in \omega\}$ be an enumeration of $\mathcal{D}$. Choose a sequence $(p_n)_{n \in \omega}$ of conditions in $\mathbb{P}$ as follows: Let $p_0 \in D_0$. Suppose for $n \in \omega$ we have chosen p_n already. Choose $p_{n+1} \leq p_n$ such that $p_{n+1} \in D_{n+1}$. This can be done since D_{n+1} is dense.

Now let
$$G := \{p \in \mathbb{P} : \exists n \in \omega (p_n \leq p)\}.$$
It is straight forward to check that G is a $\mathcal{D}$-generic filter. $\qquad\square$

Exercise 6.5. Let $(A, \leq_A)$ and $(B, \leq_B)$ countably infinite, dense linear orders without endpoints. (Recall that a linear order is dense if strictly between any two elements there is another element of the linear order.) Show that $(A, \leq_A)$ and $(B, \leq_B)$ are isomorphic.

Hint: Use the Rasiowa-Sikorski Theorem. Consider the partial $\mathbb{P}$ order of isomorphisms between finite subsets of A and B, ordered by reverse inclusion. Find a countable family $\mathcal{D}$ of dense subsets of $\mathbb{P}$ such that for every $\mathcal{D}$-generic filter $G \subseteq \mathbb{P}$ the function $\bigcup G$ is an isomorphism from A to B. It might help to take another look at Exercise 6.3.

6.2. **Generic extensions.** Our general assumption is that ZFC is consistent. In order to show that ZFC+¬CH is consistent it is enough to show that every finite set of sentences from ZFC+¬CH is consistent.

We assume that V satisfies all axioms of ZFC. We show that for every finite subset F of ZFC+¬CH there is a finite subset F' of ZFC such that is M is a countable transitive model of F', then there is a countable transitive model $M[G]$ of F. M and $M[G]$ will have the same ordinals and $M \subseteq M[G]$.

The construction of $M[G]$ is independent of the particular set F, i.e., we will simply assume that M is a countable transitive model of all of ZFC and then construct a model $M[G]$ of all of ZFC+¬CH from it. In order to verify that $M[G]$ satisfies F we will have used the fact, that M satisfies a certain finite set F' of axioms of ZFC.

Now let M be a countable transitive model of ZFC and let $\mathbb{P}$ be a partial order in M. For every $D \in M$ being a dense subset of $\mathbb{P}$ is absolute over M. Since M is countable, M contains only countably many dense subsets of $\mathbb{P}$. By the Rasiowa-Sikorski Theorem, there is a filter $G \subseteq \mathbb{P}$ such that G intersect all the dense subsets of $\mathbb{P}$ that are elements of M. Such a filter is $\mathbb{P}$-generic over M.

Exercise 6.6. Let M be a countable transitive model of ZFC and let $(\mathbb{P}, \leq) \in M$ be a partial order with the property that every $p \in \mathbb{P}$ has at least two incompatible extensions. Show that no filter $G \subseteq \mathbb{P}$ that is $\mathbb{P}$-generic over M is actually an element of M.

Hint: Given a filter $G \in M$, find a dense subset $D \in M$ that is disjoint from G.

The model $M[G]$ will be the smallest transitive model of ZFC such that $M \cup \{G\} \subseteq M[G]$. The elements of $M[G]$ coded by *names* in M that will be decoded into elements of $M[G]$ using the generic filter G.

Definition 6.7. A set τ is a $\mathbb{P}$-*name* if it is a set of pairs and moreover, for every pair $(\sigma, p) \in \tau$, p is an element of $\mathbb{P}$ and σ is a $\mathbb{P}$-name. Let $M^{\mathbb{P}}$ be the class of all $\mathbb{P}$-names in M.

Note that the definition of names is done by recursion over $\in$ and is simple enough to be absolute over M. I.e., $\tau \in M$ is a $\mathbb{P}$-name iff it is a $\mathbb{P}$-name in V.

Definition 6.8. Let G be a $\mathbb{P}$-generic filter over M. For every $\tau \in M^{\mathbb{P}}$ let

$$\tau_G = \{\sigma_G : \exists p \in G((\sigma, p) \in \tau)\}.$$

be the *evaluation* of τ with respect to G. Let

$$M[G] = \{\tau_G : \tau \in M^{\mathbb{P}}\}.$$

The evaluations τ_G are defined by recursion over $\in$. This definition takes place in V. However, the definition is absolute over transitive models of a sufficiently large fragment of ZFC.

Lemma 6.9. *If N is a transitive model of ZFC such that $M \cup \{G\} \subseteq N$, then $M[G] \subseteq N$.*

In order to show that M is a subset of $M[G]$, for every $x \in M$ we have to find a name $\tau \in M$ such that $x = \tau_G$.

Definition 6.10. For every x let $\check{x} = \{(\check{y}, 1_{\mathbb{P}}) : y \in x\}$ be the *canonical name* for x.

Lemma 6.11. *For all $x \in M$, $\check{x}_G = x$. In particular, $M \subseteq M[G]$.*

Proof. Observe that $1_{\mathbb{P}} \in G$. Now using induction over $\in$,

$$\check{x}_G = \{\check{y}_G : (\check{y}, 1_{\mathbb{P}}) \in \check{x}\} = \{y : y \in x\} = x.$$

$\square$

Next we show that $G \in M[G]$. We have to come up with a name for G.

Lemma 6.12. *Let* $\Gamma = \{(\check{p}, p) : p \in \mathbb{P}\}$. *Then* $\Gamma_G = G$.

Proof.

$$\Gamma_G = \{\check{p}_G : p \in G\} = \{p : p \in G\} = G$$

$\square$

Let us collect some properties of $M[G]$.

Lemma 6.13. *a)* $M[G]$ *is transitive.*
b) For all $\tau \in M^{\mathbb{P}}$, $\mathrm{rk}(\tau_G) \leq \mathrm{rk}(\tau)$.
c) $\mathrm{Ord} \cap M = \mathrm{Ord} \cap M[G]$

Proof. For a) let $y \in M[G]$ and $x \in y$. Then there is some name $\dot{y} \in M^{\mathbb{P}}$ such that $\dot{y}_G = y$. By the definition of $\dot{y}_G$, there is $(\dot{x}, p) \in \dot{y}$ such that $x = \dot{x}_G$ and $p \in G$. But that means that $x = \dot{x}_G \in M[G]$.

b) follows by a straight forward $\in$-induction.

For c) first observe that $\mathrm{Ord} \cap M \subseteq \mathrm{Ord} \cap M[G]$ by Lemma 6.11. On the other hand, If $\alpha \in \mathrm{Ord} \cap M[G]$, then there is a name $\dot{\alpha} \in M^{\mathbb{P}}$ such that $\dot{\alpha}_G = \alpha$. By b),

$$\alpha = \mathrm{rk}(\alpha) \leq \mathrm{rk}(\dot{\alpha}) \in \mathrm{Ord} \cap M.$$

Since $M[G]$ is transitive, $\alpha \in M$. It follows that $\mathrm{Ord} \cap M[G] \subseteq \mathrm{Ord} \cap M$. $\square$

The easier part of the proof that $M[G]$ satisfies ZFC is

Lemma 6.14. $M[G]$ *satisfies Foundation, Extensionality, Infinity, Pairing and Union.*

Proof. Foundation is automatic since $\in$ is well-founded in V. Extensionality is satisfied since $M[G]$ is transitive. Infinity holds since $\omega \in M \subseteq M[G]$. For Pairing let $a, b \in M[G]$. Choose names $\sigma, \tau \in M^{\mathbb{P}}$ such that $a = \sigma_G$ and $b = \tau_G$. Now $\eta = \{(\sigma, 1_{\mathbb{P}}), (\tau, 1_{\mathbb{P}})\}$ is a name and $\eta_G = \{\sigma_G, \tau_G\} = \{a, b\}$.

For Union let $F \in M[G]$ and let $\tau \in M^{\mathbb{P}}$ be a name such that $\tau_G = F$. Let

$$\sigma = \{(\eta, 1_{\mathbb{P}}) : \exists p, q \in \mathbb{P} \exists \pi \in M^{\mathbb{P}}((\pi, p) \in \tau \wedge (\eta, q) \in \pi)\}.$$

Obviously, $\sigma \in M^{\mathbb{P}}$.

We show that $\bigcup F \subseteq \sigma_G$. Let $a \in \bigcup F$. Then there is $b \in F$ such that $a \in b$. It follows that there are $\pi, \eta \in M^{\mathbb{P}}$ and $p, q \in G$ such that $b = \pi_G$, $a = \eta_G$, $(\eta, q) \in \pi$ and $(\pi, p) \in \tau$. By the definition of σ, $(\eta, 1_{\mathbb{P}}) \in \sigma$ and hence $a \in \sigma_G$. This shows Union. $\square$

Exercise 6.15. Assume we already know that $M[G]$ satisfies ZF. Show that $M[G]$ satisfies AC.

Hint: Since M satisfies AC, every name can be well-ordered.

Before we introduce the tools needed to verify the rest of ZFC in $M[G]$, we collect some additional data on generic filters.

Definition 6.16. A subset D of a partial order $\mathbb{P}$ is *predense* if the set $\{p \in \mathbb{P} : \exists q \in D(p \leq q)\}$ is dense. D is *predense below* $p \in \mathbb{P}$ if the set $\{q \in \mathbb{P} : \exists r \in D(q \leq r)\}$ is dense below p. A set $O \subseteq \mathbb{P}$ is *open* if for all $p \in O$ and all $q \leq p$ we have $q \in O$.

A good example of predense sets are maximal antichains (maximal with respect to $\subseteq$). Recall that $A \subseteq \mathbb{P}$ is an antichain if any two elements of A are incompatible.

Exercise 6.17. Use Zorn's Lemma to show that every antichain of $\mathbb{P}$ is contained in a maximal one.

Now let $A \subseteq \mathbb{P}$ be a maximal antichain. We show that A is predense. For this we have to show that the set $D = \{p \in \mathbb{P} : \exists q \in A(p \leq q)\}$ is dense in $\mathbb{P}$. So, let $r \in \mathbb{P}$. Since A is a maximal antichain, either $r \in A$ and hence $r \in D$ or $A \cup \{r\}$ fails to be an antichain. In the latter case, there is $p \in A$ such that r and p are compatible. Let q be a common extension of r and p. Now $q \leq r$ and $q \in D$. This shows that indeed, D is dense in $\mathbb{P}$. Hence A is predense in $\mathbb{P}$.

Exercise 6.18. Let $D \subseteq \mathbb{P}$ be dense and let $A \subseteq D$ be an antichain that is maximal among all antichains that are subsets of D. Show that A is a maximal antichain in $\mathbb{P}$.

Lemma 6.19. *Let M be a countable transitive model of ZFC, $\mathbb{P} \in M$ a partial order and $G \subseteq \mathbb{P}$ a filter.*

a) If G is generic over M and $p \in \mathbb{P}$, then the following holds:

$$p \in G \quad \leftrightarrow \quad \forall q \in G(p \not\perp q)$$

b) The following are equivalent:

(1) G is generic over M.
(2) For every $D \in M$ that is predense in $\mathbb{P}$, $G \cap D \neq \emptyset$.
(3) For every $D \in M$ that is dense and open in $\mathbb{P}$, $G \cap D \neq \emptyset$.

c) For every $p \in \mathbb{P}$ the following are equivalent:

(1) G is generic over M and $p \in G$.
(2) For every $D \in M$ that is dense below p, $G \cap D \neq \emptyset$.
(3) For every $D \in M$ that is predense below p, $G \cap D \neq \emptyset$.

Proof. a) Obviously, if $p \in G$, then p is compatible with all elements of G. Now assume that p is compatible with all elements of G. Consider the set $D = \{q \in \mathbb{P} : q \leq p \vee q \perp p\}$. D is dense in $\mathbb{P}$:

Let $r \in \mathbb{P}$. If $r \perp p$, then $r \in D$. If $r \not\perp p$, then there is $q \in \mathbb{P}$ such that $q \leq r, p$. But now $q \in D$ and hence r has an extension in D. This shows that D is dense.

Since $p, \mathbb{P} \in M$, $D \in M$. Hence G intersects D. But since all elements of G are compatible with p, the only way that G can intersect D is that G contains some q with $q \leq p$. But then $p \in G$.

b) (1) $\Rightarrow$ (3) and (2) $\Rightarrow$ (1) are trivial. Now assume (3) and let $D \in M$ be predense in $\mathbb{P}$. Let $E = \{p \in \mathbb{P} : \exists q \in D(p \leq q)\}$. Note that E is definable from D and $\mathbb{P}$ and thus $E \in M$. Since D is predense, E is dense in $\mathbb{P}$. It is easily checked that E is open. By (3), there is $p \in G \cap E$. By the definition of E, there is $q \in D$ such that $p \leq q$. Since G is a filter, $q \in G$. Hence G intersects D. This shows (2).

c) The equivalence of (2) and (3) follows using the same arguments as for the equivalence of (1) and (2) in b). Now assume either (2) or (3). Consider the set $D = \{q \in \mathbb{P} : q \leq p\}$. Clearly, D is dense below p. Hence G intersects D. Hence G contains some condition $\leq p$. Hence G contains p. This shows (1).

Now assume (1) and let $D \in M$ be dense below p. Let $E = \{q \in \mathbb{P} : (q \in D \wedge q \leq p) \vee q \perp p\}$. It is easily checked that E is dense in $\mathbb{P}$. Since $p, \mathbb{P}, D \in M$, $E \in M$. By genericity of G there is $q \in G \cap E$. Since $p \in G$ and since G is a filter, $q \not\perp p$. By the definition of E, $q \in D$. Hence G intersects D. This shows (2). $\qquad\square$

6.3. **The forcing relation.** We need a method to talk about truth in $M[G]$ from the perspective of M. This is provided by the *forcing relation* $\Vdash$ ("forces"). On the left hand side of this relation we have conditions in our fixed partial order $\mathbb{P}$. On the right hand side we have formulas of the *forcing language*. The forcing language consists of expressions of the form $\varphi(\tau_1, \ldots, \tau_n)$ where $\varphi(x_1, \ldots, x_n)$ is a formula in the language of set theory and at every free occurence of x_i, x_i has been substituted by the $\mathbb{P}$-name τ_i.

Definition 6.20. Let $p \in \mathbb{P}$, let $\varphi(x_1, \ldots, x_n)$ be a formula in the language of set theory and let $\tau_1, \ldots, \tau_n$ be $\mathbb{P}$-names. Then

$$p \Vdash \varphi(\tau_1, \ldots, \tau_n)$$

iff for all $\mathbb{P}$-generic filters G over M with $p \in G$,

$$M[G] \models \varphi((\tau_1)_G, \ldots, (\tau_n)_G).$$

The relation $\Vdash$ turns out to be a definable class in M. This is surprising since M does not have any knowledge about generic filters over M. The goal of this subsection is to show the definability of $\Vdash$ in M.

Definition 6.21. For a formula $\varphi(\tau_1, \ldots, \tau_n)$ of the forcing language of M let

$$[\![\varphi(\tau_1, \ldots, \tau_n)]\!] = \{p \in \mathbb{P} : p \Vdash \varphi(\tau_1, \ldots, \tau_n)\}$$

be the *truth value* of $\varphi(\tau_1, \ldots, \tau_n)$.

Exercise 6.22. a) Show that for every formula $\varphi(\tau_1, \ldots, \tau_n)$ in the forcing language the truthvalue $[\![\varphi(\tau_1, \ldots, \tau_n)]\!]$ is an open subset of $\mathbb{P}$.

b) Let $\varphi(\tau_1, \ldots, \tau_n)$ be as above, $p \in \mathbb{P}$ and assume that $[\![\varphi(\tau_1, \ldots, \tau_n)]\!]$ is pre-dense below p. Show that $p \in [\![\varphi(\tau_1, \ldots, \tau_n)]\!]$.

Hint: For b) use Lemma 6.19.

Note that our definition is not the standard definition of truth values in forcing. Typically, truth values are only defined if the partial order $\mathbb{P}$ is a complete Boolean algebra.

Definition 6.23. A Boolean algebra is is a partial order $\mathbb{B}$ with the following properties:

  (1) $\mathbb{B}$ has a largest element 1 and a smallest element 0.
  (2) Any two elements $a, b \in \mathbb{B}$ have a largest common lower bound $a \wedge b$ and a smallest common upper bound $a \vee b$.
  (3) Every $a \in \mathbb{B}$ has a *complement* $\neg a$ such that $a \vee \neg a = 1$ and $a \wedge \neg a = 0$.
  (4) For all $a, b, c \in \mathbb{B}$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

A Boolean algebra $\mathbb{B}$ is *complete* if every set $A \subseteq \mathbb{B}$ has a least upper bound $\bigvee A$ and a greatest lower bound $\bigwedge A$.

If $\mathbb{B}$ is a Boolean algebra, then $A \subseteq \mathbb{B}$ is a *subalgebra* of $\mathbb{B}$ if it contains 0 and 1 and is closed under $\vee$, $\wedge$ and $\neg$.

The simplest examples of Boolean algebras are the *power set algebras* $(\mathcal{P}(X), \subseteq)$ where $\wedge$ is intersection, $\vee$ union and $\neg$ actual complementation relative to the set X. It can be shown that every Boolean algebra is isomorphic to a subalgebra of a power set algebra.

If a Boolean algebra $\mathbb{B}$ is to be used for forcing purposes, we consider the partial order $\mathbb{P} = \mathbb{B} \setminus \{0\}$ instead. The traditional definition of the truth value of a formula $\varphi(\tau_1, \ldots, \tau_n)$ in a complete Boolean algebra $\mathbb{B}$ is

$$[\![\varphi(\tau_1, \ldots, \tau_n)]\!] = \bigvee \{a \in \mathbb{B} : a \Vdash \varphi(\tau_1, \ldots, \tau_n)\}.$$

We will however stick to our definition of truth values in Definition 6.21 and show later that our truth values actually are the appropriate elements of a certain complete Boolean algebra, namely the *completion* of the partial order $\mathbb{P}$ that we are forcing with.

In order to show the definability of $\Vdash$ in M it is certainly enough to show that the map

$$\varphi(\tau_1, \ldots, \tau_n) \mapsto [\![\varphi(\tau_1, \ldots, \tau_n)]\!]$$

is definable in M. In M, we will define an approximation $[\![\varphi(\tau_1, \ldots, \tau_n)]\!]^*$ of $[\![\varphi(\tau_1, \ldots, \tau_n)]\!]$ and then show that the two sets are actually the same.

For the following definitions we pretend to live inside M.

Definition 6.24. For $A \subseteq \mathbb{P}$ let

$$\operatorname{reg}(A) = \{p \in \mathbb{P} : A \text{ is predense below } p\}$$

be the *regularization* of A. A is *regular open* if $A = \operatorname{reg}(A)$.

For $A, B \subseteq \mathbb{P}$ let

$$A \vee B = \operatorname{reg}(A \cup B), \quad A \wedge B = \operatorname{reg}(A) \cap \operatorname{reg}(B) \text{ and } \neg A = \{p \in \mathbb{P} : \forall q \in A(p \perp q)\}.$$

For $p \in \mathbb{P}$ and $A \subseteq \mathbb{P}$ let $p \wedge A = A \wedge p = \{p\} \wedge A$ and $\neg p = \neg\{p\}$. For $\mathcal{F} \subseteq \mathcal{P}(\mathbb{P})$ let

$$\bigvee \mathcal{F} = \operatorname{reg}\left(\bigcup \mathcal{F}\right) \text{ and } \bigwedge \mathcal{F} = \bigcap\{\operatorname{reg}(A) : A \in \mathcal{F}\}.$$

Observe that for every A, $\operatorname{reg}(A)$ is open and contains every p such that $\operatorname{reg}(A)$ is predense below p. In other words, $\operatorname{reg}(A)$ is regular open. In fact, $\operatorname{reg}(A)$ is the smallest regular open superset of A.

The collection of all regular open subsets of $\mathbb{P}$ is denoted by $\operatorname{ro}(\mathbb{P})$ and is a complete Boolean algebra with respect to the partial order $\subseteq$. The algebraic operations on $\operatorname{ro}(\mathbb{P})$ are just $\vee$, $\wedge$ and $\neg$. For $\mathcal{F} \subseteq \operatorname{ro}(\mathbb{P})$, $\bigvee \mathcal{F}$ is indeed the supremum of $\mathcal{F}$ in $\operatorname{ro}(\mathbb{P})$ and $\bigwedge \mathcal{F}$ is the infimum. The smallest element of $\operatorname{ro}(\mathbb{P})$ is just $\emptyset$, the largest element is $\mathbb{P}$.

It is tempting to believe that $\operatorname{ro}(\mathbb{P})$ is a subalgebra of $\mathcal{P}(\mathbb{P})$, which in fact it typically is not because $\vee$, $\wedge$ and $\neg$ are not the same as $\cap$, $\cup$ and complementation in $\mathcal{P}(\mathbb{P})$.

The Boolean algebra $\operatorname{ro}(\mathbb{P})$ is the *completion* of $\mathbb{P}$. Via the map

$$e : \mathbb{P} \to \operatorname{ro}(\mathbb{P}); p \mapsto \operatorname{reg}(\{p\})$$

every element of $\mathbb{P}$ can be considered as an element of $\operatorname{ro}(\mathbb{P})$. This map, however, sometimes fails to be 1-1.

Exercise 6.25. a) Let $\mathcal{F} \subseteq \operatorname{ro}(\mathbb{P})$ be a family of regular open sets. Show that $\bigcap \mathcal{F}$ is regular open.

b) Let $A \subseteq \mathbb{P}$. Show that $\neg A$ is a regular open subset of $\mathbb{P}$.

Exercise 6.26. Let $e : \mathbb{P} \to \operatorname{ro}(\mathbb{P})$ be as above.

a) Show that the range of e is dense in $\operatorname{ro}(\mathbb{P})$. Here a subset D of a Boolean algebra B is *dense* in B if it is dense in $B \setminus \{0\}$ in the partial order sense.

b) $\mathbb{P}$ is *separative* if for $p, q \in \mathbb{P}$ we have

$$p = q \quad \leftrightarrow \quad \forall r \in \mathbb{P}(r \perp p \leftrightarrow r \perp q).$$

Show that e is 1-1 iff $\mathbb{P}$ is separative.

Hint: For b), first show that $e(p) = e(q)$ iff $\neg p = \neg q$.

Definition 6.27. Let σ and τ be $\mathbb{P}$-names. We define

$$[\![\sigma \in \tau]\!]^* = \bigvee\{[\![\sigma = \eta]\!]^* \wedge p : (\eta, p) \in \tau\},$$

$$[\![\sigma \subseteq \tau]\!]^* = \bigwedge\{\neg p \vee [\![\eta \in \tau]\!]^* : (\eta, p) \in \sigma\}$$

and

$$[\![\sigma = \tau]\!]^* = [\![\sigma \subseteq \tau]\!]^* \wedge [\![\tau \subseteq \sigma]\!]^*.$$

For formulas $\varphi(\sigma_1, \ldots, \sigma_n)$ and $\psi(\tau_1, \ldots, \tau_m)$ in the forcing language let

$$[\![\varphi(\sigma_1, \ldots, \sigma_n) \wedge \psi(\tau_1, \ldots, \tau_m)]\!]^* = [\![\varphi(\sigma_1, \ldots, \sigma_n)]\!]^* \wedge [\![\psi(\tau_1, \ldots, \tau_m)]\!]^*,$$

$$[\![\varphi(\sigma_1, \ldots, \sigma_n) \vee \psi(\tau_1, \ldots, \tau_m)]\!]^* = [\![\varphi(\sigma_1, \ldots, \sigma_n)]\!]^* \vee [\![\psi(\tau_1, \ldots, \tau_m)]\!]^*$$

and

$$[\![\neg\varphi(\sigma_1, \ldots, \sigma_n)]\!]^* = \neg[\![\varphi(\sigma_1, \ldots, \sigma_n)]\!]^*.$$

For a formula $\varphi(x, y_1, \ldots, y_n)$ in the language of set theory and $\mathbb{P}$-names $\tau_1, \ldots, \tau_n$ let

$$[\![\exists x \varphi(x, \tau_1, \ldots, \tau_n)]\!]^* = \bigvee \{ [\![\varphi(\sigma, \tau_1, \ldots, \tau_n)]\!]^* : \sigma \text{ is a } \mathbb{P}\text{-name}\}.$$

Note the very subtle recursion in this definition. For $\mathbb{P}$-names σ_0, σ_1, τ_0 and τ_1 let $(\sigma_0, \tau_0) R (\sigma_1, \tau_1)$ if $\mathrm{rk}(\sigma_0) < \mathrm{rk}(\sigma_1)$ and $\mathrm{rk}(\tau_0) \leq \mathrm{rk}(\tau_1)$ or if $\mathrm{rk}(\sigma_0) \leq \mathrm{rk}(\sigma_1)$ and $\mathrm{rk}(\tau_0) < \mathrm{rk}(\tau_1)$. The relation R is well-founded. $[\![\sigma = \tau]\!]^*$, $[\![\sigma \in \tau]\!]^*$ and $[\![\sigma \subseteq \tau]\!]^*$ are defined by recursion over R, where we first define $[\![\sigma \subseteq \tau]\!]^*$ and $[\![\tau \subseteq \sigma]\!]^*$ and only then $[\![\sigma = \tau]\!]^*$. The rest of Definition 6.27 is a typical recursion over the complexity of a formula. Here we consider $\sigma \subseteq \tau$ as an atomic formula.

Lemma 6.28. *Let $\varphi(\tau_1, \ldots, \tau_n)$ be a formula in the forcing language of M and let G be $\mathbb{P}$-generic over M. Then*

$$M[G] \models \varphi[(\tau_1)_G, \ldots, (\tau_n)_G] \quad \Leftrightarrow \quad G \cap [\![\varphi(\tau_1, \ldots, \tau_n)]\!]^* \neq \emptyset.$$

Proof. We will first prove this lemma for atomic formulas including formulas of the form $x \subseteq y$. We use induction over a well-founded relation, the same relation R that we used in the definition of the truth values of atomic formulas in the forcing language.

Let $\sigma, \tau \in M^{\mathbb{P}}$ and suppose that $\sigma_G \in \tau_G$. Then there are $\eta \in M^{\mathbb{P}}$ and $p \in G$ such that $(\eta, p) \in \tau$ and $\sigma_G = \eta_G$. Now $(\sigma, \eta) R (\sigma, \tau)$ and therefore, by the inductive hypothesis, there is $q \in [\![\sigma = \eta]\!]^* \cap G$. Since $p, q \in G$, there is $r \in G$ such that $r \leq p, q$. We have $r \in [\![\sigma = \eta]\!]^* \wedge p \subseteq [\![\sigma \in \tau]\!]^*$, showing that $G \cap [\![\sigma \in \tau]\!]^* \neq \emptyset$.

Now suppose that G intersects the set

$$[\![\sigma \in \tau]\!]^* = \bigvee \{ [\![\sigma = \eta]\!]^* \wedge p : (\eta, p) \in \tau\}.$$

By the definition of $\bigvee$, $\bigcup \{ [\![\sigma = \eta]\!]^* \wedge p : (\eta, p) \in \tau\}$ is predense below every element of $[\![\sigma \in \tau]\!]^*$. By the genericity of G, there is $(\eta, p) \in \tau$ such that $G \cap [\![\sigma = \eta]\!]^* \wedge p \neq \emptyset$. Now $p \in G$ and $G \cap [\![\sigma = \eta]\!]^* \neq \emptyset$. By the inductive hypotesis, $\sigma_G = \eta_G$. Since $p \in G$ we have $\eta_G \in \tau_G$. It follows that $\sigma_G \in \tau_G$.

Now let $\sigma_G \subseteq \tau_G$. Suppose $G \cap [\![\sigma \subseteq \tau]\!]^* = \emptyset$. By the genericity of G, there is $q \in G \cap \neg[\![\sigma \subseteq \tau]\!]^*$. We have

$$\neg[\![\sigma \subseteq \tau]\!]^* = \neg \bigwedge \{\neg p \vee [\![\eta \in \tau]\!]^* : (\eta, p) \in \sigma\} =$$

$$\bigvee \{\neg(\neg p \vee [\![\eta \in \tau]\!]^*) : (\eta, p) \in \sigma\} = \bigvee \{p \wedge \neg[\![\eta \in \tau]\!]^* : (\eta, p) \in \sigma\}.$$

Therefore $\bigcup \{p \wedge \neg[\![\eta \in \tau]\!]^* : (\eta, p) \in \sigma\}$ is predense below q. Hence, there is $(\eta, p) \in \sigma$ such that $G \cap p \wedge \neg[\![\eta \in \tau]\!]^* \neq \emptyset$. In particular, $p \in G$. Hence $\eta_G \in \sigma_G$. Moreover, $G \cap [\![\eta \in \tau]\!]^* = \emptyset$. By the inductive hypothesis, $\eta_G \notin \tau_G$. It follows that $\sigma \nsubseteq \tau$.

Assume $\sigma_G \nsubseteq \tau_G$. Then there is $(\eta, p) \in \sigma$ with $p \in G$ and $\eta_G \notin \tau_G$. By the inductive hypothesis, G does not intersect the set $[\![\eta \in \tau]\!]^*$. But then, by the genericity of G, G intersects $\neg[\![\eta \in \tau]\!]^*$. It follows that G intersects

$$p \wedge \neg[\![\eta \in \tau]\!]^* = \neg(\neg p \vee [\![\eta \in \tau]\!]^*).$$

Hence G is disjoint from

$$[\![\sigma \subseteq \tau]\!]^* = \bigwedge \{\neg p \vee [\![\eta \in \tau]\!]^* : (\eta, p) \in \sigma\}.$$

Now suppose that $\sigma_G = \tau_G$. Then $\sigma_G \subseteq \tau_G$ and $\tau_G \subseteq \sigma_G$. If G intersects $[\![\sigma \subseteq \tau]\!]^*$ and $[\![\tau \subseteq \sigma]\!]^*$, then it intersects $[\![\sigma = \tau]\!]^*$.

On the other hand, if G interects $[\![\sigma = \tau]\!]^*$, then it also intersects $[\![\sigma \subseteq \tau]\!]^*$ and $[\![\tau \subseteq \sigma]\!]^*$. It follows that $\sigma_G = \tau_G$. This finishes the argument for atomic formulas.

For non-atomic formulas we use a straight forward induction on the complexity. This yields no hidden traps and relies on arguments of the kind we have already used. $\square$

Using this lemma it is not hard to show

Theorem 6.29. *For all formulas $\varphi(\tau_1, \ldots, \tau_n)$ in the forcing language of M and for all $p \in \mathbb{P}$ we have $p \in [\![\varphi(\tau_1, \ldots, \tau_n)]\!]$ iff $p \in [\![\varphi(\tau_1, \ldots, \tau_n)]\!]^*$ holds in M. In particular, the relation $\Vdash$ is definable in M.*

Proof. Suppose $p \Vdash \varphi(\tau_1, \ldots, \tau_n)$. We show that $[\![\varphi(\tau_1, \ldots, \tau_n)]\!]^*$ is predense below p. Suppose not. Then there is some $q \leq p$ that is not compatible with any element of $[\![\varphi(\tau_1, \ldots, \tau_n)]\!]^*$. By the proof of the Rasiowa-Sikorski Theorem, there is a $\mathbb{P}$-generic filter G over M that contains q. Because of the choice of q, G is disjoint from $[\![\varphi(\tau_1, \ldots, \tau_n)]\!]^*$. By Lemma 6.28, $M[G]$ satisfies $\neg\varphi((\tau_1)_G, \ldots, (\tau_n)_G)$, contradicting the fact that with q also p is an element of G. This shows

$$[\![\varphi(\tau_1, \ldots, \tau_n)]\!] \subseteq [\![\varphi(\tau_1, \ldots, \tau_n)]\!]^*.$$

Now let $p \in [\![\varphi(\tau_1, \ldots, \tau_n)]\!]^*$. Suppose there is a $\mathbb{P}$-generic filter G over M with $p \in G$ such that $\varphi((\tau_1)_G, \ldots, (\tau_n)_G)$ fails in $M[G]$. By Lemma 6.28, $G \cap [\![\neg\varphi(\tau_1, \ldots, \tau_n)]\!]^* \neq \emptyset$. However, the condition p is incompatible with all elements of $[\![\neg\varphi(\tau_1, \ldots, \tau_n)]\!]^*$, a contradiction. If follows that $p \Vdash \varphi(\tau_1, \ldots, \tau_n)$. This shows

$$[\![\varphi(\tau_1, \ldots, \tau_n)]\!]^* \subseteq [\![\varphi(\tau_1, \ldots, \tau_n)]\!].$$

$\square$

Corollary 6.30. *Let G be $\mathbb{P}$-generic over M. For a formula $\varphi(\tau_1, \ldots, \tau_n)$ in the forcing language of M we have $M[G] \models \varphi((\tau_1)_G, \ldots, (\tau_n)_G)$ iff there is $p \in G$ such that $p \Vdash \varphi(\tau_1, \ldots, \tau_n)$.*

6.4. **ZFC in $M[G]$.** Having defined the forcing relation in M, we are now ready to verify the rest of ZFC in $M[G]$.

Theorem 6.31. $M[G]$ *satifies ZFC.*

Proof. The only axioms that we have not verified yet are Separation, Replacement and Power Set.

For Separation let $\varphi(x, y_1, \ldots, y_n)$ be a formula in the language of set theory and let $a, b_1, \ldots, b_n \in M[G]$. We show that

$$\{x \in a : M[G] \models \varphi(x, b_1, \ldots, b_n)\} \in M[G].$$

Let $\sigma, \tau_1, \ldots, \tau_n \in M^{\mathbb{P}}$ be such that $\sigma_G = a$ and for all $i \in \{1, \ldots, n\}$, $(\tau_i)_G = b_i$. Set

$$\eta = \{(\pi, p) : \exists q \in \mathbb{P}((\pi, q) \in \sigma \wedge p \leq q) \wedge p \Vdash \varphi(\pi, \tau_1, \ldots, \tau_n)\}.$$

Since $\Vdash$ is definable in M, we have $\eta \in M$. We show that $\eta_G = \{x \in a : M[G] \models \varphi(x, b_1, \ldots, b_n)\}$. Let $x \in \eta_G$. The there is $(\pi, p) \in \eta$ such that $\pi_G = x$ and $p \in G$. By the definition of η we have $p \Vdash \varphi(\pi, \tau_1, \ldots, \tau_n)$ and $p \leq q$ for some $q \in \mathbb{P}$ with $(\pi, q) \in \sigma$. It follows that $x = \pi_G \in \sigma_G$ and

$$M[G] \models \varphi(x, b_1, \ldots, b_n).$$

Now let $x \in a$ be such that $M[G] \models \varphi(x, b_1, \ldots, b_n)$. Then there is $(\pi, q) \in \sigma$ such that $x = \pi_G$ and $q \in G$. Moreover, there is $p \in G$ with $p \Vdash \varphi(\pi, \tau_1, \ldots, \tau_n)$. Since any two elements of G have a common extension in G, we may actually

assume $p \leq q$. Hence $(\pi, p) \in \eta$, and thus $x = \pi_G \in \eta_G$. This shows Separation in $M[G]$.

In order to show Replacement let $\varphi(x, y, z_1, \ldots, z_n)$ be a formula and let $a, b_1, \ldots, b_n \in M[G]$ such that

$$M[G] \models \forall x \in a \exists! y(\varphi(x, y, b_1, \ldots, b_n)).$$

Choose $\sigma, \tau_1, \ldots, \tau_n \in M^{\mathbb{P}}$ such that $\sigma_G = a$ and for all $i \in \{1, \ldots, n\}$, $(\tau_i)_G = b_i$. Choose a set $S \subseteq M^{\mathbb{P}}$ in M such that the following holds: for all $(\pi, p) \in \sigma$ and all $q \leq p$ with

$$q \Vdash \exists! y(\varphi(\pi, y, \tau_1, \ldots, \tau_n))$$

the set

$$\{r \leq q : \exists \eta \in S(r \Vdash \varphi(\pi, \eta, \tau_1, \ldots, \tau_n))\}$$

is dense below q. Consider the $\mathbb{P}$-name $S \times \{1\}$. We show that

$$M[G] \models \forall x \in a \exists y \in (S \times \{1\})_G(\varphi(x, y, b_1, \ldots, b_n)).$$

Let $x \in a$. Then there is $(\pi, p) \in \sigma$ such that $\pi_G = x$ and $p \in G$. Moreover, there is $q \in G$ such that $q \leq p$ and

$$q \Vdash \exists! y(\varphi(\pi, y, \tau_1, \ldots, \tau_n)).$$

By the choice of S there are $\eta \in S$ and $r \in G$ such that $r \leq q$ and $r \Vdash \varphi(\pi, \eta, \tau_1, \ldots, \tau_n)$. Hence

$$M[G] \models \varphi(x, \eta_G, b_1, \ldots, b_n),$$

and therefore

$$M[G] \models \exists y \in (S \times \{1\})_G(\varphi(x, y, b_1, \ldots, b_n)).$$

For Power Set let $a \in M[G]$. Choose $\sigma \in M^{\mathbb{P}}$ with $\sigma_G = a$. Let $A = \{\pi : \exists p \in \mathbb{P}((\pi, p) \in \sigma)\}$. For every function $f : A \to \mathcal{P}(\mathbb{P})$ let $\tau_f = \{(\pi, p) : p \in f(\pi)\}$. Put

$$\eta = \{(\tau_f, 1) : f \text{ is a function from } A \text{ to } \mathcal{P}(\mathbb{P})\}.$$

This definition is a definition in M.

We show

$$M[G] \models \forall x(x \subseteq a \to x \in \eta_G).$$

Let $x \in M[G]$ with $x \subseteq a$. Choose $\tau \in M^{\mathbb{P}}$ with $\tau_G = x$. Define $f : A \to \mathcal{P}(\mathbb{P})$ as follows: For $\pi \in A$ let $f(\pi) = \{p \in \mathbb{P} : p \Vdash \pi \in \tau\}$. Observe that f is a function in M. Clearly, $(\tau_f)_G \in \eta_G$. We show that $x = \tau_G = (\tau_f)_G$.

Let $y \in x$. Since $x \subseteq \sigma_G$ there is $(\pi, p) \in \sigma$ with $p \in G$ and $y = \pi_G$. Choose $q \leq p$ with $q \in G$ and $q \Vdash \pi \in \tau$. By the definition of f, $y = \pi_G \in (\tau_f)_G$. Now let $y \in (\tau_f)_G$. Then there is $(\pi, p) \in \tau_f$ with $y = \pi_G$ and $p \in G$. By the definition of f, $p \Vdash \pi \in \tau$, and hence $y = \pi_G \in \tau_G$. It follows that $\tau_G = (\tau_f)_G$. This shows that η_G is a superset of $(\mathcal{P}(a))^{M[G]}$. $\qquad\square$

Corollary 6.32. *If ZFC is consistent, then so is ZFC+V$\neq$L.*

Proof. Let M be a countable transitive model of ZFC and let $\mathbb{P} \in M$ a partial order such that every condition in $\mathbb{P}$ has two incompatible extensions, for instance $\mathbb{P} = \mathrm{Fn}(\omega, 2)$. Let G be $\mathbb{P}$-generic over M. By the previous theorem, $M[G]$ is a model of ZFC. Moreover, $M[G]$ is transitive and has the same ordinals as M. By the absoluteness of the definition of L, $L^{M[G]} = L^M \subseteq M$. Sice $G \notin M$ we have $L^{M[G]} \neq M[G]$ and thus $M[G]$ is a model of ZFC+V$\neq$L. $\qquad\square$

7. CH IS INDEPENDENT OF ZFC

In this section we show that ZFC neither implies nor refutes CH. We already know that ZFC does not refute CH, but we will give a forcing argument of this fact.

7.1. **Forcing CH.** Let M be a countable transitive model of ZFC. We define a partial order $\mathbb{P} \in M$ such that $1_{\mathbb{P}} \Vdash CH$.

Definition 7.1. In M let

$$\mathbb{P} = \{f : A \to \mathcal{P}(\omega) : A \text{ is a countable subset of } \aleph_1\}.$$

$\mathbb{P}$ is ordered by $\leq = \supseteq$.

Let G be $\mathbb{P}$-generic over M. In order to show that CH holds in $M[G]$, we first observe the following (in $M[G]$):

Lemma 7.2. Let $f_G = \bigcup G$. Then f_G is a function from $(\aleph_1)^M$ onto $\mathcal{P}(\omega) \cap M$.

Proof. Since any two elements of G have a common extension in G, $\bigcup G$ is a function. To see that f_G is defined on all of $(\aleph_1)^M$ and onto $\mathcal{P}(\omega) \cap M$, in M we define the following dense sets:

For every $\alpha < \aleph_1$ let $D_\alpha := \{p \in \mathbb{P} : \alpha \in \mathrm{dom}(p)\}$. For every $A \subseteq \omega$ let $D^A := \{p \in \mathbb{P} : A \in \mathrm{rng}(p)\}$. It is easily checked that the D_α and the D^A are dense in $\mathbb{P}$. Since G is generic over M, G intersects all D_α. Hence $\mathrm{dom}(f_G) = (\aleph_1)^M$. Since G also intersects all D^A, we have $\mathrm{rng}(f_G) = (\mathcal{P}(\omega))^M$. $\square$

In order to show that $M[G]$ satisfies CH, it is enough to show that $(\aleph_1)^M = (\aleph_1)^{M[G]}$ and $(\mathcal{P}(\omega))^M = (\mathcal{P}(\omega))^{M[G]}$. The first equality could fail since $(\aleph_1)^M$ might be countable in $M[G]$. I.e., $M[G]$ could contain a bijection between ω and $(\aleph_1)^M$. The second equality could fail since $M[G]$ might contain new subsets of ω. In both cases $M[G]$ would have to contain new functions from ω into the ordinals. We show that this cannot happen.

Lemma 7.3. Let $f \in M[G]$ be a map from ω into the ordinals. Then $f \in M$.

Proof. Let $\dot{f} \in M^{\mathbb{P}}$ be a name such that $\dot{f}_G = f$. Moreover, let $p \in G$ be such that

$$p \Vdash \dot{f} \text{ is a function from } \omega \text{ to } \mathrm{Ord}.$$

In M let

$$D = \{q \leq p : \exists g : \omega \to \mathrm{Ord}(q \Vdash \dot{f} = \check{g})\}.$$

By the genericity of G it is enough to show that D is dense below p.

We first observe the following: Let $q \leq p$ and let F be $\mathbb{P}$-generic over M with $q \in F$. Then $p \in F$. By the choice of p, $\dot{f}_F$ is a function from ω to the ordinals. Let $n \in \omega$. Then $\dot{f}_F(n) = \alpha$ for some ordinal α. Since M and $M[F]$ have the same ordinals, $\alpha \in M$. Hence there is $r \in F$ such that $r \Vdash \dot{f}(\check{n}) = \check{\alpha}$. (From now on we will drop several ˘'s in order to improve readability.) Since G is a filter, we can choose $r \leq q$. This shows that the set of all $r \in \mathbb{P}$ for which there is some $\alpha \in \mathrm{Ord}$ with $r \Vdash \dot{f}(n) = \alpha$ in dense below p.

From now on we argue in M. (This saves us several ^{M}'s.) A partial order $\mathbb{Q}$ is σ-*closed* if for every descending sequence $(q_n)_{n \in \omega}$ of conditions in $\mathbb{Q}$ there is a common extension $q \in \mathbb{Q}$ of the q_n.

$\mathbb{P}$ is σ-closed. Namely, let $(p_n)_{n \in \omega}$ be a descending sequence in $\mathbb{P}$. Then $p := \bigcup_{n \in \omega} p_n$ is a partial function from $\aleph_1$ to $\mathcal{P}(\omega)$ with countable domain and hence an element of $\mathbb{P}$. Clearly, p is a common extension of all the p_n.

We are now in the position to show that D is dense below p. Let $q \leq p$. Choose $q_0 \leq q$ and $\alpha_0 \in \mathrm{Ord}$ such that $q_0 \Vdash \dot{f}(0) = \alpha_0$. This is possible by the remark at the beginning of this proof. Suppose we have chosen q_n. As above, there is

$q_{n+1} \leq q_n$ and $\alpha_{n+1} \in \mathrm{Ord}$ such that $q_{n+1} \Vdash \dot{f}(n+1) = \alpha_{n+1}$. By the σ-closedness of $\mathbb{P}$, there is a common extension r of all the q_n. We show that $r \in D$.

Let $g : \omega \to \mathrm{Ord}; n \mapsto \alpha_n$. For all $n \in \omega$ we have $r \leq q_n$. In particular, $r \Vdash \dot{f}(n) = \alpha_n$ for all $n \in \omega$. Since ω is the same in all transitive models of set theory, $r \Vdash \dot{f} = \check{g}$. Hence $r \in D$. It follows that D is dense below p. $\qquad\square$

Corollary 7.4. $M[G] \models CH$

Proof. By Lemma 7.3 we have $(\mathcal{P}(\omega))^M = (\mathcal{P}(\omega))^{M[G]}$ and $(\aleph_1)^M$ is uncountable in $M[G]$. All ordinals below $(\aleph_1)^M$ are countable in M and hence in $M[G]$. It follows that $(\aleph_1)^M = (\aleph_1)^{M[G]}$. By Lemma 7.2 in $M[G]$ there is map from $(\aleph_1)^{M[G]} = (\aleph_1)^M$ onto $(\mathcal{P}(\omega))^{M[G]} = (\mathcal{P}(\omega))^M$. Hence $M[G] \models |\mathcal{P}(\omega)| \leq \aleph_1$. This it is provable in ZFC that $\mathcal{P}(\omega)$ is uncountable and $M[G]$ is a model of ZFC, we have $M[G] \models$ CH. $\qquad\square$

Exercise 7.5. Let $\mathbb{P}$ be a partial order. Consider the following two player game that lasts ω many rounds:

Let $p_0 = q_0 = 1_{\mathbb{P}}$. In the n-th round the first player choses a condition $p_{n+1} \leq q_n$ and the second player replies by chosing a condition $q_{n+1} \leq p_{n+1}$. The second player wins the game iff there is a common extension $p \in \mathbb{P}$ of the p_n.

Suppose the second player has a winning strategy for this game. Show that for every G that is $\mathbb{P}$-generic over M, $M[G]$ does not contain any new function from ω into the ordinals.

Exercise 7.6. Let $\mathbb{P} = \mathrm{Fn}(\omega, 2)$. Show that the first player has a winning strategy in the game described above.

8. Forcing ¬CH

In order to force the failure of CH, we start from a countable transitive model M of ZFC+CH and generically add at least $(\aleph_2)^M$ new subsets of ω. This is rather easily accomplished. What requires work is to show that the $\aleph_2$ of the ground model M actually remains $\aleph_2$ in the extension.

In M, let κ be a cardinal $> \aleph_1$ and let

$$\mathbb{P} = \mathrm{Fn}(\kappa \times \omega, 2) = \{p : A \to 2 : A \text{ is a finite subset of } \kappa \times \omega\}$$

be ordered by reverse inclusion.

Let G be $\mathbb{P}$-generic over M. Then $f_G = \bigcup G$ is a function from $\kappa \times \omega$ to 2. For every $\alpha \in \kappa$ let $a_\alpha = \{n \in \omega : f_G(\alpha, n) = 1\}$.

Lemma 8.1. *If $\alpha, \beta \in \kappa$ are different, then so are a_α and a_β.*

Proof. Consider the set

$$D_{\alpha,\beta} = \{p \in \mathbb{P} : \exists n \in \omega((\alpha, n), (\beta, n) \in \mathrm{dom}(p) \wedge p(\alpha, n) \neq p(\beta, n))\}.$$

Let $p \in \mathbb{P}$. Since the domain of p is finite, there is $n \in \omega$ such that neither (α, n) not (β, n) are in the domain of p. Extend p to a condition q such that $(\alpha, n), (\beta, n) \in \mathrm{dom}(q)$ and $q(\alpha, n) \neq q(\beta, n)$. Then clearly, $q \in D_{\alpha,\beta}$.

It follows that $D_{\alpha,\beta}$ is dense in $\mathbb{P}$. Hence there is $p \in G \cap D_{\alpha,\beta}$. Now $p \subseteq f_G$ and hence $f_G(\alpha, n) \neq f_G(\beta, n)$. This implies $a_\alpha \neq a_\beta$. $\qquad\square$

This shows that forcing with $\mathbb{P}$ adds κ new subsets of ω. In order to show that κ remains large in $M[G]$, we need to discuss a crucial property of the forcing notion $\mathbb{P}$.

8.1. **The countable chain condition and preservation of cardinals.**

Definition 8.2. A partial order $\mathbb{Q}$ satisfies the *countable* (anti-) *chain condition* (c.c.c.) if every antichain of $\mathbb{Q}$ is countable.

It turns out that forcing with a c.c.c. partial order does not collapse cardinals. The following is the combinatorial foundation of the proof of this fact.

Lemma 8.3. *In M, let $\mathbb{Q}$ be c.c.c. Then for every $\mathbb{Q}$-generic filter F over M and every function $f \in M[F]$ from some ordinal $\alpha \in M$ to the ordinals of M there is a function $\overline{f} \in M$ from α to the countable sets of ordinals of M such that for all $\beta < \alpha$, $f(\beta) \in \overline{f}(\beta)$.*

Proof. Let F be $\mathbb{Q}$-generic over M and let $f \in M[F]$ be a function from some ordinal α to Ord. Choose a name $\dot{f} \in M^{\mathbb{Q}}$ such that $\dot{f}_F = f$. There is $p \in F$ that forces $\dot{f}$ to be a function from α to Ord.

Let $q \leq p$ and let H be $\mathbb{Q}$-generic over M with $q \in H$. For each $\beta < \alpha$ there is an ordinal γ_β such that $\dot{f}_H(\beta) = \gamma_\beta$. This has to be forced by some $r \in H$. We say that r *decides* $\dot{f}(\beta)$. Since q and r have a common extension in F, we may chose $r \leq q$ to begin with.

This argument shows that for each $\beta < \alpha$ the set

$$D_\beta = \{r \in \mathbb{Q} : r \text{ decides } \dot{f}(\beta)\}$$

is dense below p. For each $\beta < \alpha$ let A_β be a maximal antichain below p consisting of conditions that decide $\dot{f}(\beta)$. Since D_β is dense below p, A_β is really maximal among all the antichains below p. In particular, it is predense below p. Let

$$\overline{f}(\beta) = \{\gamma : \exists r \in A_\beta (r \Vdash \dot{f}(\beta) = \gamma)\}.$$

Since $\mathbb{Q}$ is c.c.c., A_β and hence $\overline{f}(\beta)$ is countable. Since A_β is predense below p and $p \in F$, there is $r \in F$ such that r forces $\dot{f}(\beta)$ to be an element of $\overline{f}(\beta)$. Hence $\dot{f}_F(\beta) \in \overline{f}(\beta)$. $\qquad\square$

Definition 8.4. A partial order $\mathbb{Q}$ *preserves cardinals* if for every cardinal κ,

$$1_{\mathbb{Q}} \Vdash \text{``}\kappa \text{ is a cardinal''}.$$

$\mathbb{Q}$ *preserves cofinalities* if for every ordinal α and $\kappa = \mathrm{cf}(\alpha)$, $1_{\mathbb{Q}} \Vdash \kappa = \mathrm{cf}(\alpha)$.

Lemma 8.5. *If $\mathbb{Q}$ preserves cofinalities, then it preserves cardinals.*

Proof. Let F be $\mathbb{Q}$-generic over M and suppose there is a cardinal in M that ceases to be a cardinal in $M[F]$. By transfinite induction on the cardinals in M we show that all the cardinals of M are still cardinals in $M[F]$.

Clearly, $(\aleph_0)^M = (\aleph_0)^{M[F]}$. If κ is limit cardinal in M and all cardinals below κ are preserved, then in $M[F]$, κ is still the supremum of a set of cardinals and hence a cardinal.

If κ is a successor cardinal in M, then $\mathrm{cf}(\kappa) = \kappa$ in M. Since $\mathbb{Q}$ preserves cofinalities, in $M[F]$, κ is still the cofinality of an ordinal and hence a cardinal. $\quad\square$

Lemma 8.6. *If $\mathbb{Q}$ is c.c.c., then it preserves cofinalities and hence cardinals.*

Proof. Let F be $\mathbb{Q}$ generic over M. Suppose in $M[F]$, α is an ordinal and $\kappa = \mathrm{cf}(\alpha)$. Let $f : \kappa \to \alpha$ be cofinal.

If α is a successor ordinal in $M[F]$, then it is a successor ordinal in M as well. Hence we may assume that α is a limit ordinal. If α is of countable cofinality in M, then it will have the same cofinality in $M[F]$. Hence we may assume that in M the cofinality of α is uncountable.

By Lemma 8.3, in M there is a function $\overline{f}$ from κ to the countable subsets of α such that for all $\beta < \kappa$, $f(\beta) \in \overline{f}(\beta)$. Since α is of uncountable cofinality in M, for each $\beta < \alpha$ we have $\gamma(\beta) = \sup(\overline{f}(\beta)) < \alpha$.

Now for each $\beta < \alpha$, $f(\beta) \leq \gamma(\beta)$. Since f is cofinal in α, so is g. Hence in M, $\text{cf}(\alpha) \leq \kappa$. But since κ is the least size of a cofinal subset of α in $M[F]$, there is no cofinal subset of α of size $< \kappa$ in M. Therefore in M, $\kappa = \text{cf}(\alpha)$.

It follows that $\mathbb{Q}$ preserves cofinalities. $\qquad\square$

We now have to show that $\mathbb{P} = \text{Fn}(\kappa \times \omega, 2)$ is actually c.c.c. This fact is also non-trivial and can be shown using the Δ-*System Lemma*, which is pure combinatorics.

Lemma 8.7 (Δ-System Lemma). *Let $\mathcal{F}$ be an uncountable family of finite sets. Then there are a finite set r and an uncountable family $\mathcal{D} \subseteq \mathcal{F}$ such that for all distinct $s, t \in \mathcal{D}$, $s \cap t = r$. $\mathcal{D}$ is called a Δ-system with root r.*

Proof. After throwing away members of the family, we may assume that $\mathcal{F}$ is of size $\aleph_1$. Now $\bigcup \mathcal{F}$ is of size $\aleph_1$ Hence we may also assume that $\mathcal{F}$ consists of subsets of $\aleph_1$. Moreover, we may assume that all elements of $\mathcal{F}$ have the same size, say n. Let $(a_\alpha)_{\alpha, \omega_1}$ be a 1-1 enumeration of $\mathcal{F}$.

Let $f_i : \aleph_1 \to \aleph_1$, $i < n$ be functions such that for all $\alpha < \aleph_1$, $a_\alpha = \{f_i(\alpha) : i < n\}$ and $f_0(\alpha) < \cdots < f_{n-1}(\alpha)$.

Clearly, if f_i is unbounded, then for all $j < n$ with $i < j$, f_j is unbounded as well. Let $k \leq n$ be maximal such that for all $i < k$, f_i is bounded. Let $\alpha < \aleph_1$ be strictly greater than all the elements of the ranges of the f_i, $i < k$. Since α is countable, α has only countably many finite subsets. This shows that at least one of f_i is unbounded and hence $k < n$. Since f_k is unbounded, there is an uncountable set $I \subseteq \aleph_1$ such that f_k is 1-1 on I. Moreover, there is a finite set $r \subseteq \alpha$ such that $J = \{\beta \in I : \{f_i(\beta) : i < k\} = r\}$ is uncountable.

By recursion we now choose a strictly increasing sequence $(\beta_\gamma)_{\gamma < \aleph_1}$ in J such that $\max(r) < f_k(\beta_0)$ and for $\gamma < \gamma' < \aleph_1$ we have $f_{n-1}(\beta_\gamma) < f_k(\beta_{\gamma'})$. This is possible since f_k is unbounded on J.

It is easily checked that $\mathcal{D} = \{a_{\beta_\gamma} : \gamma < \aleph_1\}$ is a Δ-system with root r. $\qquad\square$

Lemma 8.8. *For every set X, $\text{Fn}(X, 2)$ is c.c.c.*

Proof. Let $A \subseteq \text{Fn}(X, 2)$ be uncountable. By the Δ-System Lemma, A has an uncountable subset B such that the supports of the elements of B form a Δ-system with some root $r \subseteq X$. Since there are only finitely many functions from r to 2, B contains two different conditions p and q that agree on r. Since the sets $\text{dom}(p) \setminus r$ and $\text{dom}(q) \setminus r$ are disjoint, $p \cup q$ is a function. It follows that p and q are compatible. Hence A is not an antichain. $\qquad\square$

Corollary 8.9. *CH fails in $M[G]$.*

Proof. Recall that G is $\text{Fn}(\kappa \times \omega, 2)$-generic over M where κ is a cardinal $> \aleph_1$ in M. Since $\text{Fn}(\kappa \times \omega, 2)$ is c.c.c., M and $M[G]$ have the same cardinals. By Lemma 8.1, ω has at least κ subsets in $M[G]$. Hence $M[G] \models \neg\text{CH}$. $\qquad\square$

8.2. **Nice names and the size of $2^{\aleph_0}$.** Let M, κ, $\mathbb{P}$ and G be as before. We want to compute the actual value of $2^{\aleph_0}$ in $M[G]$. We do this by finding a small set of $\mathbb{P}$-names such that every $a \in \mathcal{P}(\omega) \cap M[G]$ has a name in that set.

Exercise 8.10. Let $a \in M[G]$. Show that in M there is a proper class of names σ with $\sigma_G = a$.

Definition 8.11. Let $\mathbb{Q}$ be a partial order. A $\mathbb{Q}$-name σ is a *nice name for a subset of ω* if there is a family $(A_n)_{n \in \omega}$ of antichains of $\mathbb{Q}$ such that

$$\sigma = \{(\check{n}, p) : p \in A_n\} = \bigcup_{n \in \omega} (\{\check{n}\} \times A_n).$$

Lemma 8.12. *Let F be $\mathbb{Q}$-generic over M. Then for every $a \in \mathcal{P}(\omega) \cap M[F]$ there is a nice name $\sigma \in M$ for a subset of ω such that $a = \sigma_F$.*

Proof. Fix a name $\tau \in M$ such that $a = \tau_F$. For each $n \in \omega$ let A_n be a maximal antichain in the set $\{p \in \mathbb{Q} : p \Vdash n \in \tau\}$. Clearly, $\sigma = \{(\check{n}, p) : p \in A_n\}$ is a nice name for a subset of ω.

We have to verify that $\sigma_F = a$. Let $n \in \sigma_F$. Then for some $p \in A_n$, $p \in F$. By the choice of A_n, $p \Vdash n \in \tau$ and hence $n \in \tau_F = a$. This shows $\sigma_F \subseteq a$.

On the other hand, if $n \in a$, then there is $(\pi, p) \in \tau$ such that $p \in F$ and $\pi_F = n$. For some $q \in F$, $q \Vdash \pi = n$. We can choose $q \leq p$. Now $q \Vdash n \in \tau$. Since A_n is a maximal antichain in the set of conditions that force $n \in \tau$, A_n is predense below q. Since F is generic and $q \in F$, there is $r \in F \cap A_n$. Now $r \Vdash n \in \sigma$ and hence $n \in \sigma_F$. This shows $a \subseteq \sigma_F$ and hence $a = \sigma_F$. $\qquad\square$

Exercise 8.13. Recall the definition of the sets a_α, $\alpha < \kappa$, mentioned in Lemma 8.1. Write down explicitly a nice name for each a_α.

Lemma 8.14. *Let $\mathbb{Q}$ be c.c.c. Then there are at most $|\mathbb{Q}|^{\aleph_0}$ nice $\mathbb{Q}$-names for subsets of ω.*

Proof. Since $\mathbb{Q}$ is c.c.c., all antichains of $\mathbb{Q}$ are countable. Hence $\mathbb{Q}$ has at most $|\mathbb{Q}|^{\aleph_0}$ antichains. A nice name for a subset of ω is essentially just a function from ω into the set of antichains of $\mathbb{Q}$. It follows that there are at most

$$(|\mathbb{Q}|^{\aleph_0})^{\aleph_0} = |\mathbb{Q}|^{\aleph_0}$$

nice names for subsets of ω. $\qquad\square$

Theorem 8.15. *In M, let $\mathbb{P} = \mathrm{Fn}(\kappa \times \omega, 2)$. Let G be $\mathbb{P}$-generic over M. Then $M[G] \models 2^{\aleph_0} = (\kappa^{\aleph_0})^M$.*

Proof. Since κ is infinite, $(\kappa^{\aleph_0})^M \geq (2^{\aleph_0})^M$. Since $\mathbb{P}$ is c.c.c., it preserves cardinals. By Lemma 8.1, $(2^{\aleph_0})^{M[G]}$ is at least κ. Since $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}$, $(2^{\aleph_0})^{M[G]}$ is at least $(\kappa^{\aleph_0})^{M[G]}$. Clearly, $(\kappa^{\aleph_0})^M \leq (\kappa^{\aleph_0})^{M[G]}$ On the other hand, in M there are at most $\kappa^{\aleph_0}$ nice names for subsets of ω and hence $|\mathcal{P}(\omega)|^{M[G]} \leq (\kappa^{\aleph_0})^M$ and the theorem follows. $\qquad\square$

Corollary 8.16. *Let M, G and κ be as above. If M satisfies GCH and $\mathrm{cf}(\kappa) > \aleph_0$, then in $M[G]$, $2^{\aleph_0} = \kappa$. If M satisfies GCH but $\mathrm{cf}(\kappa) = \aleph_0$, then in $M[G]$, $2^{\aleph_0} = \kappa^+$.*

Proof. The corollary follows from the previous theorem and the fact that under GCH we have $\kappa^{\aleph_0} = \kappa$ if $\mathrm{cf}(\kappa) > \aleph_0$ and $\kappa^{\aleph_0} = \kappa^+$ if κ is an infinite cardinal of countable cofinality. $\qquad\square$

Exercise 8.17. Prove the statement about the size of $\kappa^{\aleph_0}$ under GCH used in the proof of the previous corollary.

9. Martin's Axiom

Having produced models of ZFC in which CH fails, there are several natural questions.

1. Let $\kappa < 2^{\aleph_0}$ be a cardinal. Is $2^\kappa \leq 2^{\aleph_0}$?
2. How many measure zero sets are needed to cover the real line?
3. Let X be a topological space. $A \subseteq X$ is *nowhere dense* if the closure of A has an empty interior. The Baire Category Theorem says (in particular) that $\mathbb{R}$ is not the union of countably many nowhere dense sets. But how many nowhere dense sets are needed to cover all of $\mathbb{R}$?
4. A family $\mathcal{A} \subseteq \mathcal{P}(\omega)$ is *almost disjoint* if all $A, B \in \mathcal{A}$ with $A \neq B$ have a finite intersection. An easy application of Zorn's Lemma shows that every almost disjoint family of subsets of ω is contained in a maximal one. What is the minimal size of an infinite maximal almost disjoint family? (An easy argument shows that no countably infinite almost disjoint family is maximal.)

All of these questions have an obvious answer under CH. *Martin's Axiom* also answers all these questions, but is consistent with ¬CH. In fact, MA is only interesting if CH fails since under CH it does not say anything new as it follows from CH.

Definition 9.1. Let κ be a cardinal. MA_κ says that for every c.c.c. partial order $\mathbb{P}$ and every family $\mathcal{D}$ of size κ of dense subsets of $\mathbb{P}$ there is a $\mathcal{D}$-generic filter $G \subseteq \mathbb{P}$.

Martin's Axiom (MA) is the statement

$$\forall \kappa < 2^{\aleph_0} (\text{MA}_\kappa).$$

9.1. **Martin's Axiom and Souslin's Hypothesis.** The original motivation to introduce Martin's Axiom lies in *Souslin's Hypothesis*. A linear order $(L, \leq)$ is *c.c.c.* if there is no uncountable family of pairwise disjoint open intervals of L. L is *separable* if it has a countable dense subset. L is connected if it is not the union of two disjoint open subsets.

It is relatively easy to show that every connected separable linear order without endpoints is isomorphic to $\mathbb{R}$. *Suslins Hypothesis (SH)* is the statement that every connected c.c.c. linear order without endpoints is isomorphic to $\mathbb{R}$. CH neither implies nor refutes SH. (Both directions of this independence result are due to Jensen.) SH fails in L. The consistency proof of MA+¬CH is a relatively straight forward generalization generalization of Solovay's and Tennenbaum's proof of the consistency of SH. Martin's name is attached to the axiom because he observed that the consistency proof of SH could be adapted to show the consistency of something much stronger, namely of MA with an arbitrarily large size of $2^{\aleph_0}$

We now show how $\mathrm{MA}_{\aleph_1}$ implies SH. A *Souslin line* is a connected linear order without endpoints that is c.c.c. but not separable. Since every separable connected linear order without endpoints is isomorphic to the real line, SH holds and only if there is no Souslin line.

Definition 9.2. A partial order $(T, \leq)$ is a *tree* if for all $t \in T$ the set $\{s \in T : s \leq t\}$ is well ordered. If T is a tree and $t \in T$, then the *height* $\mathrm{ht}_T(t)$ of t in T is the order type of the set $\{s \in T : s < t\}$, i.e., the unique ordinal α such that $(\alpha, \in)$ is isomorphic to $(\{s \in T : s < t\}, <)$. For an ordinal α, the α-th level $\mathrm{Lev}_\alpha(T)$ of T is the set of all *nodes* $t \in T$ of height α.

A *branch* of a tree T is a maximal chain in T. An *antichain* in a tree T is a family of pairwise incomparable elements of the tree. A tree is *Souslin* if it is uncountable and has neither uncountable chains nor antichains.

Lemma 9.3. *If there is a Souslin line, then there is a Souslin tree.*

Actually the existence of a c.c.c. linear order that is not separable implies the existence of a Souslin line by roughly the same proof as below. Connectedness simplifies the proof a tiny little bit. The main information that connectedness gives us is that L has to be a dense linear order, i.e., if $a, b \in L$ are such that $a < b$, then (a, b) is nonempty (and in fact infinite).

Proof. Let $(L, \leq)$ be a Souslin line. The Souslin tree T that we are going to construct will consist of nonempty open intervals in L ordered by reverse inclusion. By recursion on $\alpha \in \mathrm{Ord}$ we define the α-th level of the tree T.

Let $\mathrm{Lev}_0(T) = \{L\}$. We consider L as a nonempty open interval of L. Suppose we have constructed the β-th level of T and $\alpha = \beta + 1$. For each interval $I \in \mathrm{Lev}_\beta(T)$ let A_I be a an infinite maximal disjoint family of open intervals contained in I. This is possible since by connectedness every nonempty open interval of L has at least two disjoint nonempty open subintervals. Let

$$\mathrm{Lev}_\alpha(T) = \bigcup \{A_I : I \in \mathrm{Lev}_\beta(T)\}.$$

Now assume that α is a limit ordinal and for all $\beta < \alpha$ we have already defined $\mathrm{Lev}_\beta(T)$. Let $\mathrm{Lev}_\alpha(T)$ be a maximal of pairwise disjoint, nonempty open intervals I with the property that for every $\beta < \alpha$ there is $J \in \mathrm{Lev}_\beta(T)$ with $I \subseteq J$. This finishes the definition of T. Obviously, the levels of T are eventually empty.

Every antichain of T is a family of pairwise disjoint, nonempty open intervals of L. Since L is c.c.c., every antichain of T is countable. In particular, every level of T is countable.

Now suppose that T has an uncountable chain. Since T is a tree, every chain of T is wellordered. Hence, if T has an uncountable chain, it has a chain of the form $(I_\alpha)_{\alpha \in \aleph_1}$, where $I_\beta \subseteq I_\alpha$ if $\alpha < \beta$. Now the sequence of left endpoints of the I_α has an uncountable increasing subsequence or the sequence of right endpoints of the I_α has an uncountable decreasing subsequence. Without loss of generality assume the former and let $(a_\alpha)_{\alpha \in \aleph_1}$ be a strictly increasing sequence in L. Then $((a_\alpha, a_{\alpha+1}))_{\alpha \in \aleph_1}$ is an uncountable family of pairwise disjoint, nonempty open intervals in L, a contradiction. It follows that T has no uncountable chains. Note that this implies that $\mathrm{Lev}_{\aleph_1}(T)$ is empty.

It remains to show that T is uncountable. Let D be the collection of all the endpoints of the intervals $I \in T$ that are not $+\infty$ or $-\infty$. We claim that D is dense in L. Let $a, b \in L$ be such that $a < b$. It is enough to find some interval $I \in T$ that intersects (a, b) but is not a superset of (a, b) since in this case (a, b) has to contain an endpoint of I.

Let α be minimal with the property that (a, b) is disjoint from every element of $\mathrm{Lev}_\alpha(T)$.

We first observe that α is a limit ordinal. Otherwise $\alpha = \beta + 1$ for some ordinal β and there is $I \in \mathrm{Lev}_\beta(T)$ such that I has a nonempty intersection with (a, b). But now A_I was chosen to be a maximal family of paiwise disjoint, nonempty open subintervals of I. Since $I \cap (a, b)$ is a nonempty open subinterval of I, there is $J \in A_I \subseteq \mathrm{Lev}_\alpha(T)$ such that J intersects (a, b), a contradiction.

By the choice of α, for every $\beta < \alpha$, there is $I \in \mathrm{Lev}_\beta(T)$ with $(a, b) \cap I \neq \emptyset$. If some of these I's intersects (a, b) but is not a superset of (a, b), we are done. Hence we may assume that for each $\beta < \alpha$ there is $I \in \mathrm{Lev}_\beta(T)$ such that $(a, b) \subseteq I$. But by the definition of $\mathrm{Lev}_\alpha(T)$, this means that some $J \in \mathrm{Lev}_\alpha(T)$ intersect (a, b), contradicting the choice of α.

We have thus found a dense subset of L of size at most $|T|$. Since L is not separable, T is uncountable. It follows that T is a Souslin tree. $\square$

The converse of this lemma is also true: if there is a Souslin tree, then there is a Souslin line.

Theorem 9.4. $MA_{\aleph_1}$ *implies SH.*

Proof. We show that under $\mathrm{MA}_{\aleph_1}$ there are no Souslin trees. Assume there is a Souslin tree $(T, \leq)$. We have to prune the tree a bit. Namely, we remove all those nodes $t \in T$ such that for some $\alpha < \aleph_1$, there is no $s \in \mathrm{Lev}_\alpha(T)$ with $t \leq s$. Let T' denote the pruned tree. Now for every t in T and every $\alpha < \aleph_1$ with $\alpha > \mathrm{ht}_T(t)$ there is a node $s \in T'$ of height α such that $t \leq s$.

If not, then for some $t \in T'$ and $\alpha < \aleph_1$ with $\alpha > \mathrm{ht}_T(t)$, t has no successors at the α's level of T'. But this implies that all successors of t in $\mathrm{Lev}_\alpha(T)$ have only countably many successors in T. It follows that t has only countably many successors in T, a contradiction since $t \in T'$.

Now let $\mathbb{P}$ be the tree T', but ordered by the relation $\geq$. Now antichains in the tree T' correspond to antichains in the partial order $\mathbb{P}$. Since with T also T' has only countable antichains, $\mathbb{P}$ is c.c.c.

Since every $t \in T'$ has successors of every countable height, for every $\alpha < \aleph_1$ the set $D_\alpha = \{t \in T' : \mathrm{ht}_{T'}(t) > \alpha\}$ is dense in $\mathbb{P}$. By $\mathrm{MA}_{\aleph_1}$ there is a $(D_\alpha)_{\alpha < \aleph_1}$-generic filter $G \subseteq \mathbb{P}$. It is easily checked that G is an uncountable chain in T' and hence in T. A contradiction. $\square$

9.2. **The Baire Category Theorem and Martin's Axiom.** In its strongest form the Baire Category Theorem states that no complete metric space and no compact space is the union of countably many nowhere dense sets. We concentrate on compact spaces.

A topological space X is c.c.c. if every family of pairwise disjoint open subsets of X is countable.

Theorem 9.5. *MA is equivalent to the statement "no c.c.c. compact space is the union of fewer than $2^{\aleph_0}$ nowhere dense sets".*

The proof of this theorem needs a couple of lemmas. Before we start proving it, we point out an important consequence.

Corollary 9.6. *Under MA, $\mathbb{R}$ is not the union of fewer than $2^{\aleph_0}$ nowhere dense sets.*

Proof. $\mathbb{R}$ is not compact, but $[0, 1]$ is and $\mathbb{R}$ is homeomorphic to $(0, 1)$. A subset of $(0, 1)$ is nowhere dense in $(0, 1)$ iff it is nowhere dense in $[0, 1]$. The singletons $\{0\}$ and $\{1\}$ are nowhere dense in $[0, 1]$. It follows that the number of nowhere dense subsets of $[0, 1]$ needed to cover $[0, 1]$ is the same as the number of nowhere dense subsets of $(0, 1)$ needed to cover $(0, 1)$. In particular, $(0, 1)$ and therefore $\mathbb{R}$ cannot be covered by fewer than $2^{\aleph_0}$ nowhere dense sets. $\square$

Our first step in the proof of Theorem 9.5 is to associate every Boolean algebra with a compact space. This connection between Boolean algebras and certain compact spaces is known as *Stone Duality*.

Definition 9.7. Let A be a Boolean algebra and $F \subseteq A$. We say that F is an *ultrafilter* of A iff F is a maximal filter in the partial order $A \setminus \{0\}$ or equivalently, if F is a filter in $A \setminus \{0\}$ and for each $a \in A$ either $a \in F$ or $\neg a \in F$.

Let $\mathrm{Ult}(A)$ denote the set of ultrafilters of A topologized by declaring the sets of the form $[a] = \{F \in \mathrm{Ult}(A) : a \in F\}$, $a \in A$, as open. I.e., a subset of $\mathrm{Ult}(A)$ is open iff it is a union of sets of the form $[a]$. We call the sets $[a]$ *basic open*.

Exercise 9.8. A set $S \subseteq A$ has the *finite intersection property* if for all n and all $a_1, \ldots, a_n \in A$, $a_1 \wedge \cdots \wedge a_n \neq 0$. By Zorn's Lemma, every set with the finite intersection property is contained in a maximal set with the finite intersection property. Show that a maximal set $S \subseteq A$ with the finite intersection property is an ultrafilter of A.

Lemma 9.9. *For every Boolean algebra A, $\mathrm{Ult}(A)$ is a compact space, the* Stone space *of A.*

Proof. We first show that Stone spaces are Hausdorff, i.e., for two distinct points $x, y \in \mathrm{Ult}(A)$ there are disjoint open sets $U, V \subseteq \mathrm{Ult}(A)$ such that $x \in U$ and $y \in V$.

Let $x, y \in \mathrm{Ult}(A)$ be such that $x \neq y$. Then there is $a \in A$ such that $a \in x$ and $a \notin y$ or vice versa. Without loss of generality we assume the first. Since y is an ultrafilter, $\neg a \in y$. Now $[a]$ and $[\neg a]$ are disjoint open sets, the first containing x, the second containing y. This shows Hausdorffness.

Now let $\mathcal{O}$ be an open cover of $\mathrm{Ult}(A)$. For every $x \in \mathrm{Ult}(A)$ choose $a_x \in A$ such that for some $U_x \in \mathcal{O}$ we have $x \in [a_x] \subseteq U_x$. Clearly, $\mathrm{Ult}(A) = \bigcup_{x \in \mathrm{Ult}(A)}[a_x]$. If there are finitely many points $x_1, \ldots, x_n \in \mathrm{Ult}(A)$ such that $\mathrm{Ult}(A) = [a_{x_1}] \cup \cdots \cup [a_{x_n}]$, then $\{U_{x_1}, \ldots, U_{x_n}\}$ is a finite subcover of $\mathcal{O}$ and we are done.

Suppose there are not finitely many x such that the corresponding $[a_x]$ union up to $\mathrm{Ult}(A)$. In this case the family $\{\mathrm{Ult}(A) \setminus [a_x] : x \in \mathrm{Ult}(A)\}$ has the finite intersection property, i.e., no finite intersection of sets from the family is empty. This easily translates to the finite intersection property of $\{\neg a_x : x \in \mathrm{Ult}(A)\}$. By the previous exercise there is an ultrafilter y of A that extends $\{\neg a_x : x \in \mathrm{Ult}(A)\}$. It is easily checked that $y \notin \bigcup_{x \in \mathrm{Ult}(A)}[a_x]$, a contradiction. $\square$

Exercise 9.10. Let A be a Boolean algebra. For each $a \in A$ let $D_a = \{b \in A : b \leq a \vee b \perp a\}$. Then each D_a is a dense subset of A. If $F \subseteq G$ is a $(D_a)_{a \in A}$-generic filter, then F is an ultrafilter.

Lemma 9.11. *Let A be a Boolean algebra and $S \subseteq \mathrm{Ult}(A)$. If S is nowhere dense in $\mathrm{Ult}(A)$, then the set*

$$D_S = \{a \in A \setminus \{0\} : [a] \cap S = \emptyset\}$$

is dense in A.

On the other hand, if D is a dense subset of A, then the set

$$\{x \in \mathrm{Ult}(A) : x \notin \bigcup\{[a] : a \in D\}\}$$

is nowhere dense in $\mathrm{Ult}(A)$.

Proof. Let S be nowhere dense. Taking the closure of S we can assume that S is closed. Let $a \in A \setminus \{0\}$. Since S is closed and nowhere dense, $[a] \not\subseteq S$. Hence $[a] \setminus S$ is a nonempty open subset of $\mathrm{Ult}(A)$. Since the topology on $\mathrm{Ult}(A)$ is generated by the basic open sets, there is $b \in A \setminus \{0\}$ such that $[b] \subseteq [a] \setminus S$ and thus $b \in D_S$ and $b \leq a$. This shows the density of D_S.

Now let D be a dense subset of A and let $U_D = \bigcup\{[a] : a \in D\}$. As a union of open sets, U_D is open. In order to show that $\mathrm{Ult}(A) \setminus U_D$ is nowhere dense, it is enough to show that U_D is dense in $\mathrm{Ult}(A)$. Let $V \subseteq \mathrm{Ult}(A)$ be nonempty and open. Then there is $a \in A \setminus \{0\}$ such that $[a] \subseteq V$. By the density of D, there is $b \in D$ such that $b \leq a$. Now clearly $[b] \subseteq V \cap U_D$. This shows that U_D is dense in $\mathrm{Ult}(A)$. $\square$

We need yet another observation for the proof of Theorem 9.5 that will also be useful when we show the consistency of Martin's Axiom with the negation of CH.

Lemma 9.12. *Let κ be a infinite cardinal. Then MA_κ holds iff MA_κ holds restricted to ccc partial orders of size κ.*

Proof. We show only the nontrivial direction. Let $(\mathbb{P}, \leq)$ be a ccc partial order and let $\mathcal{D}$ be a family of κ dense subsets of $\mathbb{P}$.

Let λ be sufficiently large and choose an elementary submodel M of V_λ of size λ such that $\mathcal{D} \subseteq M$ and $(\mathcal{P}, \leq) \in M$. We consider the partial order $\mathbb{Q} = M \cap \mathbb{P}$. Like $\mathbb{P}$, $\mathbb{Q}$ is ccc. For each $q \in \mathbb{Q}$ and each $D \in \mathcal{D}$, M believes that there is some $p \in D$ such that $p \leq q$. It follows that for all $q \in \mathbb{Q}$ and all $D \in \mathcal{D}$ there is $p \in M \cap D$ such that $p \leq q$. Hence the sets $D \cap M$, $D \in \mathcal{D}$, are dense in $\mathbb{Q}$. By MA_κ restricted to partial orders of size κ, there is a filter $F \subseteq \mathbb{P}$ that is generic for the collection $\{D \cap M : D \in \mathcal{D}\}$ of dense subsets of $\mathbb{Q}$. F extends to a filter $G \subseteq \mathbb{P}$. G is $\mathcal{D}$ generic. $\square$

Proof of Theorem 9.5. Assume MA and let X be a c.c.c. compact space. Let $\mathbb{P}$ denote the collection of all nonempty open subsets of X ordered by inclusion. Since X is c.c.c., so is $\mathbb{P}$. Let $\mathcal{F}$ be a collection of fewer than $2^{\aleph_0}$ nowhere dense subsets of X. We may assume that each member of $\mathcal{F}$ is a closed set. For each $S \in \mathcal{F}$ let

$$D_S = \{U \in \mathbb{P} : \mathrm{cl}(U) \cap S = \emptyset\}.$$

Let $S \in \mathcal{F}$ and let $U \subseteq X$ be nonempty and open. Since S is closed and nowhere dense, $U \setminus S$ is nonempty and open. Let $V \subseteq X$ be nonempty, open and such that $\mathrm{cl}(V) \subseteq U \setminus S$. By the definition of D_S, $V \in D_S$. It follows that D_S is dense in $\mathbb{P}$.

By MA, there is a $(D_S)_{S \in \mathcal{F}}$-generic filter $G \subseteq \mathbb{P}$. Let $T = \bigcap\{\mathrm{cl}(U) : U \in G\}$. Since G has the finite intersection property and X is compact, $T \neq \emptyset$. By the genericity of G, T is disjoint from every $S \in \mathcal{F}$, showing that $\mathcal{F}$ does not cover X.

On the other hand, assume that no c.c.c. compact space is the union of fewer than $2^{\aleph_0}$ nowhere dense sets. By Lemma 9.12, in order to prove Martin's Axiom, it is enough to prove Martin's Axiom restricted to partial orders of size $< 2^{\aleph_0}$. Let $\mathbb{P}$ be a partial order of size $< 2^{\aleph_0}$. Let $A = \mathrm{ro}(\mathbb{P})$ and $X = \mathrm{Ult}(A)$.

Claim 9.13. X is c.c.c.

Let $\mathcal{A}$ be a family of pairwise disjoint, nonempty open subsets of X. We may assume that every element of $\mathcal{A}$ is of the form $[a]$ for some $a \in A$. We may further assume that every element of $\mathcal{A}$ is of the form $[a]$ where $a = \mathrm{reg}\, p$ for some $p \in \mathcal{P}$. Since the elements of $\mathcal{A}$ are pairwise disjoint, the corresponding elements of $\mathbb{P}$ are pairwise incompatible. Since $\mathbb{P}$ is c.c.c., $\mathcal{A}$ is countable. This shows the claim.

Now let $\mathcal{D}$ be a collection of fewer than $2^{\aleph_0}$ dense subsets of $\mathbb{P}$. Since $\mathbb{P}$ is of size $< 2^{\aleph_0}$, we may assume that for all $p, q \in \mathbb{P}$, the set

$$D_{p,q} = \{r \in \mathbb{P} : r \leq p, q \text{ or } r \perp p \text{ or } r \perp q\}$$

is in $\mathcal{D}$. Let $e : \mathbb{P} \to \mathrm{ro}(\mathbb{P})$ be the natural embedding. Since $e[\mathbb{P}]$ is dense in $\mathrm{ro}(\mathbb{P})$, the images of the $D \in \mathcal{D}$ in $\mathrm{ro}(\mathbb{P})$ are also dense. It follows that for each $D \in \mathcal{D}$ the set $S_D = X \setminus \bigcup\{[e(p)] : p \in D\}$ is nowhere dense in X.

By our assumption, X is not the union of the S_D, $D \in \mathcal{D}$. It follows that there is an ultrafilter F of A that is not in any of the sets S_D, $D \in \mathcal{D}$. Let $G = \{p \in \mathbb{P} : e(p) \in F\}$. Hence, if $D \in \mathcal{D}$, $F \in \bigcup\{[e(p)] : p \in D\}$. But this implies that there is some $p \in D$ such that $e(p) \in F$. By the definition of G, $p \in G$. This shows that G has a nonempty intersection with D. We still have to show that G is in fact a filter. It is clear that if $p \in G$ and $p \leq q$, then $q \in G$.

Now let $p, q \in G$. If $p \perp q$, then $e(p)$ and $e(q)$ are incompatible in $\mathrm{ro}(\mathbb{P})$. Hence $e(p)$ and $e(q)$ cannot both be elements of F. It follows that any two elements of G are compatible. Since $D_{p,q} \in \mathcal{D}$, there is $r \in G \cap D_{p,q}$. Since any two elements of G are compatible, r is compatible to both p and q. But in this case, $r \leq p, q$. This shows that G is a $\mathcal{D}$-generic filter, proving that MA holds for ccc partial orders of size $< 2^{\aleph_0}$. $\qquad\square$

9.3. More consequences of MA.
We first observe that Martin's Axiom implies that the real line is not covered by less than continuum many sets of measure 0.

Theorem 9.14. MA_κ *implies that $\mathbb{R}$ is not the union of κ sets of measure 0.*

Proof. First observe that it is enough to show that $[0, 1]$ is not the union of κ sets of measure 0. Let $\mathbb{P}$ be the partial order of all measurable subsets of $[0, 1]$ of measure > 0 ordered by inclusion. We first show that $\mathbb{P}$ is ccc.

Let $A \subseteq \mathbb{P}$ be an uncountable antichain. Then for distinct $p, q \in A$, $p \cap q$ is of measure 0. For each $n \in \omega$ let

$$A_n = \left\{p \in A : \text{the measure of } p \text{ is at least } \tfrac{1}{2^{-n}}\right\}.$$

Now $A = \bigcup_{n \in \omega} A_n$ and hence for some $n \in \omega$, A_n is uncountable. Let $(p_i)_{i \in \omega}$ be a 1-1-sequence in A_n. For each $k \in \omega$ let $q_k = p_k \setminus \bigcup_{i < k} p_k$. Now the q_k are pairwise disjoint and the measure of each q_k is equal to the measure of p_k since p_k and q_k only differ by a set of measure 0.

The q_k are pairwise disjoint and of measure at least $\tfrac{1}{2^{-n}}$. It follows that their union is of infinite measure, contradicting the fact that each q_k is a subset of $[0, 1]$. It follows that $\mathbb{P}$ is indeed ccc.

For a set $N \subseteq [0, 1]$ of measure 0 let

$$D_N = \{p \in \mathbb{P} : \mathrm{cl}(p) \cap N = \emptyset\}.$$

Here $\mathrm{cl}(p)$ denotes the closure of the set p. Since N is of measure 0, for every $p \in \mathbb{P}$, $p \setminus N$ is of positive measure. Every set of positive measure contains a closed set of positive measure. It follows that D_N is dense in $\mathbb{P}$.

Now let $G \subseteq \mathbb{P}$ be a filter that intersects D_N. Since G is a filter, it is closed under finite intersections. Since $[0, 1]$ is compact, every family of closed subsets of $[0, 1]$ with the finite intersection property has a nonempty intersection. Hence $\bigcap\{\mathrm{cl}(p) : p \in G\}$ is nonempty. Since G intersects D_N, $\bigcap\{\mathrm{cl}(p) : p \in G\}$ is disjoint from N.

If $\mathcal{N}$ is a family of size κ of sets of measure 0 and MA_κ holds, then there is a filter $G \subseteq \mathbb{P}$ that intersects each D_N, $N \in \mathcal{N}$. Now $\bigcap\{\mathrm{cl}(p) : p \in G\}$ is a nonempty subset of $[0, 1]$ that is disjoint from $\bigcup \mathcal{N}$. In particular, the family $\mathcal{N}$ does not cover $[0, 1]$. $\qquad\square$

The next goal is to prove that for infinite κ, MA_κ implies that $2^\kappa = 2^{\aleph_0}$. Let us we look at two similar forcing notions, one of which will be used for the above statement.

Definition 9.15. a) *Hechler forcing* $\mathbb{H}$ is the partial order with conditions of the form $p = (f_p, F_p)$ where for some $n \in \omega$, $f_p : n \to \omega$ and F_p is a finite set of functions from ω to ω. For $p, q \in \mathbb{H}$, let $p \leq q$ if $f_q \subseteq f_p$ and for all $n \in \mathrm{dom}(f_p) \setminus \mathrm{dom}(f_q)$ and all $f \in F_q$, $f_p(n) \geq f(n)$.

b) Let $\mathcal{A}$ be an infinite set of subsets of ω that pairwise have finite intersection, i.e., an *almost disjoint family*. *Almost disjoint forcing* $\mathbb{AD}$ is the partial order with conditions of the form $p = (f_p, \mathcal{A}_p)$ where for some $n \in \omega$, $f_p : n \to 2$ and $\mathcal{A}_p$ is a finite subset of $\mathcal{A}$. For $p, q \in \mathbb{AD}$, let $p \leq q$ if $f_q \subseteq f_p$ and for all $A \in \mathcal{A}_q$ and all $n \in (A \cap \mathrm{dom}(f_p)) \setminus \mathrm{dom}(f_q)$, $f_p(n) = 0$. Observe that $\mathbb{AD}$ depends on the choice of the almost disjoint family $\mathcal{A}$.

We will show that both almost disjoint forcing and Hechler forcing are ccc. In fact, they satisfy a stronger property.

Definition 9.16. A subset S of a partial order $\mathcal{P}$ is *centered* if any finitely many elements of S have a common lower bound in $\mathbb{P}$. A partial order $\mathcal{P}$ is *σ-centered* if it is the union of countably centered set.

Lemma 9.17. *Every σ-centered partial order is ccc.*

Lemma 9.18. *Both Hechler forcing and almost disjoint forcing are σ-centered.*

Proof. In both cases it is enough to observe that there are only countably many first components of conditions and the set of conditions with a fixed first component is centered. $\square$

Definition 9.19. A family $\mathcal{F} \subseteq \omega^\omega$ is *bounded* if there is $g : \omega \to \omega$ such that for all $f \in \mathcal{F}$ and all but finitely many $n \in \omega$, $f(n) \leq g(n)$.

Theorem 9.20. *Let κ be an infinite cardinal and assume MA_κ. Then no almost disjoint family of size κ of subsets of ω is maximal almost disjoint. Every family of size κ of functions from ω to ω is bounded.*

Proof. Let $\mathcal{A}$ be an almost disjoint family of size κ of subsets of ω. Let $\mathbb{AD}$ be the almost disjoint forcing with respect to $\mathcal{A}$. For each $A \in \mathcal{A}$, $D_A = \{p \in \mathbb{AD} : A \in \mathcal{A}_p\}$ is dense in $\mathbb{AD}$. Also, for each $n \in \omega$, the set $D^n = \{p \in \mathbb{AD} : \exists m \in \mathrm{dom}(f_p) \setminus n (f_p(m) = 1)\}$ is dense in $\mathbb{AD}$.

By MA_κ, let $G \subseteq \mathbb{AD}$ be a filter that intersects all $D_A, A \in \mathcal{A}$, and all D^n, $n \in \omega$. Let $f = \bigcup_{p \in G} f_p$. Then $f : \omega \to 2$ is the characteristic function of an infinite set $B \subseteq \omega$. We show that B is almost disjoint from all $A \in \mathcal{A}$ and hence $\mathcal{A}$ is not a maximal almost disjoint family. It is enough to prove the following:

Claim 9.21. Let $p \in G \cap D_A$. Then $A \cap B \subseteq \mathrm{dom}(f_p)$.

For the proof of the claim let $n \in B \setminus \mathrm{dom}(f_p)$. Then $f(n) = 1$ and hence there is $q \in G$ such that $n \in \mathrm{dom}(f_q)$ and $f_q(q) = 1$. Wlog we may assume that $q \leq p$. By the definition of $\leq$ and since $A \in \mathcal{A}_p$, $n \notin A$, finishing the proof of the claim.

The proof of the corresponding statement for families of functions is almost the same using Hechler forcing. $\square$

We now show that for every infinite cardinal κ, MA_κ implies $2^\kappa = 2^{\aleph_0}$. In order to do this, we have to code subsets of κ by subsets of ω. This is done by *almost disjoint coding*, which is due to Solovay.

Fix an almost disjoint family $\mathcal{A}$ of size κ of subsets of ω consisting of infinite sets. Instead of subsets of κ, we code subsets of $\mathcal{A}$ by subsets of ω, in the following way:

Lemma 9.22. *Assume MA_κ. Then for each $\mathcal{B} \subseteq \mathcal{A}$ there is $C \subseteq \omega$ such that for all $B \in \mathcal{B}$, $B \cap C$ is finite and for all $A \in \mathcal{A} \setminus \mathcal{B}$, $C \cap A$ is infinite. In other words, C is almost disjoint from every element of $\mathcal{B}$ and not almost disjoint from every element of $\mathcal{A} \setminus \mathcal{B}$.*

Proof. We use almost disjoint forcing for the almost disjoint family $\mathcal{B}$. Let for $n \in \omega$ and $A \in \mathcal{B}$ let D^n and D_A be the dense sets of almost disjoint forcing defined in the proof of Theorem 9.20. For all $A \in \mathcal{A} \setminus \mathcal{B}$ and all $n \in \omega$ let

$$E_A^n = \{p \in \mathbb{AD} : \exists m \in A \setminus n(m \in \mathrm{dom}(f_p) \wedge f_p(m) = 1)\}.$$

Then each of the sets E_A^n is dense in $\mathbb{AD}$.

Now let $G \subseteq \mathbb{AD}$ be a filter that intersects all the dense sets D^n, $n \in \omega$, the sets D_A, $A \in \mathcal{B}$, and E_A^n, $n \in \omega$ and $A \in \mathcal{A} \setminus \mathcal{B}$. Let $f = \bigcup_{p \in G} f_p$ and let $C = f^{-1}(1)$. Then C has the desired properties. $\qquad\square$

Corollary 9.23. *If κ is an infinite cardinal and MA_κ holds, then $2^{\aleph_0} = 2^\kappa$.*

9.4. **Iterated forcing.** We are going to show the consistency of MA with ¬CH by means of *iterated forcing*. The strategy is as follows: we start with a countable transitive model M of GCH and construct an increasing sequence $(M_\alpha)_{\alpha \leq (\aleph_2)^M}$ of models of set theory and a sequence $(G_\alpha)_{\alpha < (\aleph_2)^M}$ such that $M_0 = M$ and for all $\alpha < (\aleph_2)^M$, G_α is $\mathbb{Q}_\alpha$-generic over M_α where $\mathbb{Q}_\alpha \in M_\alpha$ is a partial order and $M_{\alpha+1} = M_\alpha[G_\alpha]$. For each $\alpha < (\aleph_2)^M$,

$$M_\alpha \models \text{``}\mathbb{Q}_\alpha \text{ is a c.c.c. partial order of size } \aleph_1\text{''}.$$

Most of the $\mathbb{Q}_\alpha$ add new reals, all the M_α, $\alpha < (\aleph_2)^M$ satisfy CH, the final model $M_{(\aleph_2)^M}$ satisfies $2^{\aleph_0} = \aleph_2$ and no cardinals are collapsed in the process. We choose $\mathbb{Q}_\alpha$ in such a way that in the final model the following holds: whenever $\mathbb{P}$ is a c.c.c. forcing of size $\aleph_1$ and $\mathcal{D}$ is a family of fewer than $\aleph_2$ dense subsets of $\mathbb{P}$, then there is $\alpha < (\aleph_2)^M = \aleph_2$ such that $\mathbb{P} = \mathbb{Q}_\alpha$ and $\mathcal{D} \subseteq M_\alpha$. In particular, G_α, which is an element of $M_{(\aleph_2)^M}$, intersects every $D \in \mathcal{D}$, showing that there is a $\mathcal{D}$-generic filter of $\mathbb{P}$. By Lemma 9.12, this is enough to show MA in $M_{(\aleph_2)^M}$.

Our strategy has one major problem: If $\alpha \leq (\aleph_2)^M$ is a limit ordinal, how do we define M_α? It is tempting to choose M_α simply as the union of the previous M_β, $\beta < \alpha$. However, there is no reason why this union should be a model of ZFC. A strategy that works, however, is to define a single forcing notion $\mathbb{Q}$ in the ground model M such that every $\mathbb{Q}$-generic filter G over M codes a sequence $(G_\alpha)_{\alpha < (\aleph_2)^M}$ of filters and a sequence $(M_\alpha)_{\alpha \leq (\aleph_2)^M}$ of models of set theory as above.

Let us first consider the case where we want to iterate just two forcings. Let $\mathbb{P}$ be a partial order in M and let G be $\mathbb{P}$-generic over M. Let $\mathbb{Q}$ be a forcing notion in $M[G]$ and let F be $\mathbb{Q}$-generic over $M[G]$. Then $M[G, F] = M[G][F]$ is a model of set theory. We want to represent $M[G, F]$ as a single generic extension of M with respect to a certain forcing notion in M. The problem is that $\mathbb{Q}$ might not be an element of M. Hence, from the point of view of M, we can access $\mathbb{Q}$ only in terms of a $\mathbb{P}$-name $\dot{\mathbb{Q}}$. For simplicity, we would like to assume that $1_\mathbb{P}$ forces that $\dot{\mathbb{Q}}$ is a partial order. Moreover, typically the partial order $\mathbb{Q}$ has a simple definition in $M[G]$ such as "$\mathbb{Q}$ is the partial order of all closed subsets of $\mathbb{R}$ of positive measure". We would like to have a name $\dot{\mathbb{Q}}$ that is forced by $1_\mathbb{P}$ to satisfy this definition.

All this is made possible by the *Existential Completeness Lemma*.

Lemma 9.24 (Existential Completeness Lemma, respectively Maximality Principle)**.** *Let $\varphi(x, y_1, \ldots, y_n)$ be a formula in the language of set theory. Let $\mathbb{P}$ be a partial order, $\tau_1, \ldots, \tau_n$ $\mathbb{P}$-names and $p \in \mathbb{P}$. Suppose that*

$$p \Vdash \exists x \varphi(x, \tau_1, \ldots, \tau_n).$$

Then there is a $\mathbb{P}$-name σ such that

$$p \Vdash \varphi(\sigma, \tau_1, \ldots, \tau_n).$$

The proof of this lemma uses the following sublemma:

Lemma 9.25. *Let $\mathbb{P}$ be a partial order, $A \subseteq \mathbb{P}$ an antichain and $(\sigma_p)_{p \in A}$ a family of $\mathbb{P}$-names. Then there is a $\mathbb{P}$-name σ such that for all $p \in A$, $p \Vdash \sigma = \sigma_p$.*

Proof. Let

$$\sigma = \{(\eta, r) : \exists p \in A \exists q \in \mathbb{P}(r \leq p \wedge r \leq q \wedge (\eta, q) \in \sigma_p)\}.$$

Now, if $p \in A$, we claim that $p \Vdash \sigma = \sigma_p$.

Let G be generic over the ground model with $p \in G$. Let $(\eta, r) \in \sigma$ be such that $r \in G$ and $\eta_G = x$. Since A is an antichain, p is the unique element of A that is in G. Hence $r \leq p$. By the definition of σ there is $q \in \mathbb{P}$ such that $r \leq q$ and $(\eta, q) \in \sigma_p$. Now $q \in G$ and hence $x = \eta_G \in (\sigma_p)_G$. This shows $\sigma_G \subseteq (\sigma_p)_G$.

On the other hand, let $x \in (\sigma_p)_G$. Fix $(\eta, q) \in \sigma_p$ such that $q \in G$ and $\eta_G = x$. since p and q are both in G, there is a common extension $r \in G$ of both p and q. By the definition of σ, $(\eta, r) \in \sigma$ and hence $x = \eta_G \in \sigma_G$. This shows $(\sigma_p)_G \subseteq \sigma_G$. $\square$

Proof of the Existential Completeness Lemma. By the definition of the truthvalue $[\![\exists x \varphi(x, \tau_1, \ldots, \tau_n)]\!]$ the set

$$D = \{q \leq p : \exists \eta \in V^{\mathbb{P}}(q \Vdash \varphi(\eta, \tau_1, \ldots, \tau_n))\}$$

is predense below p. Since D is open, it is actually dense below p. Choose a maximal antichain A in D. For each $q \in A$ choose a name η_q such that $q \Vdash \varphi(\eta_q, \tau_1, \ldots, \tau_n)$. By the previous lemma there is a name σ such that for all $q \in A$, $q \Vdash \sigma = \eta_q$. Since A is predense below p,

$$p \Vdash \varphi(\sigma, \tau_1, \ldots, \tau_n).$$

$\square$

Definition 9.26. Let $\mathbb{P}$ be a partial order and let $\dot{\mathbb{Q}}$ be a $\mathbb{P}$-name for a partial order, i.e., a $\mathbb{P}$-name such that $1_{\mathbb{P}}$ forces $\dot{\mathbb{Q}}$ to be a partial order. The *two-step iteration* of $\mathbb{P}$ and $\dot{\mathbb{Q}}$ is the partial order $\mathbb{P} * \dot{\mathbb{Q}}$ consisting of all pairs $(p, \dot{q})$ where p is a condition in $\mathbb{P}$ and $\dot{q}$ is a $\mathbb{P}$-name such that $p \Vdash \dot{q} \in \dot{\mathbb{Q}}$.

Let $\leq_{\mathbb{P}}$ denote the order on $\mathbb{P}$ and let $\dot{\leq}_{\mathbb{Q}}$ be a $\mathbb{P}$-name for the order on $\dot{\mathbb{Q}}$. We define the order $\leq$ on $\mathbb{P} * \dot{\mathbb{Q}}$ as follows: $(p_1, \dot{q}_1) \leq (p_2, \dot{q}_2)$ iff $p_1 \leq_{\mathbb{P}} p_2$ and

$$p_1 \Vdash \dot{q}_1 \dot{\leq}_{\mathbb{Q}} \dot{q}_2.$$

We will drop the subscripts $\mathbb{P}$ and $\mathbb{Q}$ if they are clear from the context.

Observe that with this definition of the iteration of $\mathbb{P}$ and $\dot{\mathbb{Q}}$, $\mathbb{P} * \dot{\mathbb{Q}}$ turns out to be a proper class. Hence we redefine $\mathbb{P} * \dot{\mathbb{Q}}$ as

$$\{(p, \dot{q}) \in \mathbb{P} * \dot{\mathbb{Q}} : \mathrm{rk}(\dot{q}) < \mathrm{rk}(\mathbb{P}) + \omega, \mathrm{rk}(\dot{\mathbb{Q}}) + \omega\}$$

even though this definition obviously lacks the elegance of the first definition. Now whenever $p \in \mathbb{P}$ and $\dot{q}$ is a $\mathbb{P}$-name such that $p \Vdash \dot{q} \in \dot{\mathbb{Q}}$, then there is a $\mathbb{P}$-name $\dot{r}$ such that $(p, \dot{r}) \in \mathbb{P} * \dot{\mathbb{Q}}$ and $p \Vdash \dot{r} = \dot{q}$. Whenever we choose a name for an element of $\dot{\mathbb{Q}}$ we implicitly assume that we only consider names of rank $< \mathrm{rk}(\mathbb{P}) + \omega, \mathrm{rk}(\dot{\mathbb{Q}}) + \omega$.

Now let $\dot{1}_{\mathbb{Q}}$ be a name for the largest element of $\dot{\mathbb{Q}}$. Then obviously,

$$i : \mathbb{P} \to \mathbb{P} * \dot{\mathbb{Q}} : p \mapsto (p, \dot{1}_{\mathbb{P}})$$

is an embedding of partial orders. If H is $\mathbb{P} * \dot{\mathbb{Q}}$-generic over the ground model M, We define $G = i^{-1}[H]$ and $F = \{\dot{q}_G : \exists p \in G((p, \dot{q}) \in H)\}$.

Lemma 9.27. G is $\mathbb{P}$-generic over M and F is $\dot{\mathbb{Q}}_G$-generic over $M[G]$

Proof. It is easily checked that G is a filter. Let $D \in M$ be a dense subset of $\mathbb{P}$. Then the set $D' = \{(p, \dot{q}) \in \mathbb{P} * \dot{\mathbb{Q}} : p \in D\}$ is dense in $\mathbb{P} * \dot{\mathbb{Q}}$ and hence there is $(p, \dot{q}) \in H \cap D'$. Since $(p, \dot{q}) \leq (p, \dot{1}_{\mathbb{Q}})$, $(p, \dot{1}_{\mathbb{Q}}) \in H$ and thus $p \in G \cap D$.

We now show that F is a filter in $\dot{\mathbb{Q}}_G$. Suppose that $\dot{q}_G \in F$ and $\dot{r}_G \in \dot{\mathbb{Q}}_G$ is such $\dot{q}_G \leq \dot{r}_G$. Then there is $p \in G$ such that $p \Vdash \dot{q} \leq \dot{r}$. Since $p \in G$, $(p, \dot{1}_{\mathbb{Q}}) \in H$. Since $\dot{q}_G \in F$, there is $p' \in \mathbb{P}$ such that $(p', \dot{q}) \in H$. Since H is a filter, $(p, \dot{1}_{\mathbb{Q}})$ and $(p', \dot{q})$ have a common extension $(p'', \dot{s})$ in H. Now $p'' \Vdash \dot{q} \leq \dot{r}$ and $p'' \Vdash \dot{s} \leq \dot{q}$. It follows that $p'' \Vdash \dot{s} \leq \dot{r}$. Since $p'' \leq p'$ we have $(p'', \dot{s}) \leq (p'', \dot{r})$ and thus $\dot{r}_G \in F$. A similar argument shows that any two elements of F have a common extension in F.

Now let $D \in M[G]$ be a dense subset of $\dot{\mathbb{Q}}_G$. There is a $\mathbb{P}$-name $\dot{D} \in M$ for D. By the Maximality Principle we may assume that $1_{\mathbb{P}}$ forces $\dot{D}$ to be a dense subset of $\dot{\mathbb{Q}}$. Consider the set

$$D' = \{(p, \dot{q}) \in \mathbb{P} * \dot{\mathbb{Q}} : p \Vdash \dot{q} \in \dot{D}\}.$$

This set is dense in $\mathbb{P} * \dot{\mathbb{Q}}$:

Let $(p, \dot{q})$ be an element of $\mathbb{P} * \dot{\mathbb{Q}}$. Since $\dot{D}$ is forced to be dense in $\dot{Q}$ and by the Maximality Principle, there is a name $\dot{r}$ such that p forces $\dot{r}$ to be an element of $\dot{D}$ that is an extension of $\dot{q}$. Now $(p, \dot{r}) \leq (p, \dot{q})$ and $p \in D'$. It follows that D' is dense in $\mathbb{P} * \dot{\mathbb{Q}}$.

Since H is $\mathbb{P} * \dot{\mathbb{Q}}$-generic over M, there is $(p, \dot{q}) \in D' \cap H$. Now $(p, \dot{1}_{\mathbb{Q}}) \in H$ and thus $p \in G$. By the definition of D', $p \Vdash \dot{q} \in \dot{D}$. By the definition of F, $\dot{q}_G \in F$. It follows that $D \cap F \neq \emptyset$. Therefore F is generic over $M[G]$. $\square$

Lemma 9.28. *If* M, $\mathbb{P}$ *and* $\dot{\mathbb{Q}}$ *are as above,* G *is* $\mathbb{P}$-*generic over* M *and* F *is* $\dot{\mathbb{Q}}_G$-*generic over* $M[G]$, *then*

$$H = G * F = \{(p, \dot{q}) : p \in G \wedge \dot{q}_G \in F\}$$

is $\mathbb{P} * \dot{\mathbb{Q}}$-*generic over* M.

Proof. Exercise $\square$

Lemma 9.29. *If* $\mathbb{P}$ *is c.c.c. and* $1_{\mathbb{P}} \Vdash$ *"$\dot{\mathbb{Q}}$ is c.c.c.", then* $\mathbb{P} * \dot{\mathbb{Q}}$ *is c.c.c.*

Proof. Assume there is a subset $\{(p_\alpha, \dot{q}_\alpha) : \alpha < \omega_1\}$ of $\mathbb{P} * \dot{\mathbb{Q}}$ such that $(p_\alpha, \dot{q}_\alpha)$ is incompatible with $(p_\beta, \dot{q}_\beta)$ if $\alpha \neq \beta$. Consider the name

$$\sigma = \{(\check{\alpha}, p_\alpha) : \alpha < \omega_1\}.$$

Since $\mathbb{P}$ is c.c.c., the ω_1 of the ground model remains ω_1 in the generic extension by $\mathbb{P}$.

Now let G be $\mathbb{P}$-generic over M and let $\alpha, \beta \in \sigma_G$ be distinct. Suppose $(\dot{q}_\alpha)_G$ and $(\dot{q}_\beta)_G$ are compatible. Then there is a $\mathbb{P}$-name $\dot{r}$ for a condition in $\dot{\mathbb{Q}}$ that is a common extension of $(\dot{q}_\alpha)_G$ and $(\dot{q}_\beta)_G$. Some $p \in G$ forces that $\dot{r}$ is a common extension of $\dot{q}_\alpha$ and $\dot{q}_\beta$. We may assume that p is a common extension of p_α and p_β. Now $(p, \dot{r})$ is a common extension of $(p_\alpha, \dot{q}_\alpha)$ and $(p_\beta, \dot{q}_\beta)$, a contradiction.

It follows that the $(\dot{q}_\alpha)_G$ are pairwise incompatible. Since $\dot{\mathbb{Q}}_G$ is c.c.c., it follows that σ_G is countable. Hence the supremum of σ_G is a countable ordinal.

We now forget about the particular filter G again and choose a $\mathbb{P}$-name $\dot{\beta} \in M$ for the supremum of σ. Since $\mathbb{P}$ is c.c.c., there is a countable set $C \subseteq \omega_1$ such that $1_{\mathbb{P}}$ forces $\dot{\beta}$ to be an element $\check{C}$.

Let γ be the supremum of C. By the choice of $\dot{\beta}$, $1_{\mathbb{P}} \Vdash \dot{\beta} \leq \check{\gamma}$. But by the definition of $\dot{\beta}$ this means that no p_α with $\alpha > \gamma$ can be an element of a $\mathbb{P}$-generic filter over M, a contradiction. $\qquad\square$

9.5. **Long iterations.** We will now define iterations of infinite length.

Definition 9.30. Let δ be an ordinal. $((\mathbb{P}_\alpha)_{\alpha \leq \delta}, (\dot{\mathbb{Q}}_\beta)_{\beta < \delta})$ is a *finite support iteration length δ* if the following conditions are satisfied:
   (1) For every $\alpha \leq \delta$, $\mathbb{P}_\alpha$ is a partial order consisting of sequences of length α. In particular, $\mathbb{P}_0$ is the trivial partial order $\{\emptyset\}$.
   (2) If $\alpha < \beta \leq \delta$ and $p \in \mathbb{P}_\beta$, then $p \restriction \alpha \in \mathbb{P}_\alpha$.
   (3) For every $\alpha < \delta$, $\dot{\mathbb{Q}}_\alpha$ is a $\mathbb{P}_\alpha$-name for a partial order and $\mathbb{P}_{\alpha+1} = \mathbb{P}_\alpha * \dot{\mathbb{Q}}_\alpha$. Since $\mathbb{P}_\alpha$ consists of sequences of length α, it is natural to consider $\mathbb{P}_\alpha * \dot{\mathbb{Q}}_\alpha$ as consisting of sequences of length $\alpha + 1$.
   (4) If $\beta \leq \delta$ is a limit ordinal, then $\mathbb{P}_\beta$ consists of all sequences p of length β such that the support
   $$\operatorname{supt}(p) = \{\alpha < \beta : p(\alpha) \neq \dot{1}_{\mathbb{Q}_\alpha}\}$$
   of p is finite and for all $\alpha < \beta$, $p \restriction \alpha \in \mathbb{P}_\alpha$.
   (5) If $\leq$ denotes the order on $\mathbb{P}_\beta$ and $p, q \in \mathbb{P}_\beta$, then $p \leq q$ if for all $\alpha < \beta$, $p \restriction \alpha \Vdash p(\alpha) \dot{\leq}_\alpha q(\alpha)$ where $\dot{\leq}_\alpha$ is a name for the order on $\dot{\mathbb{Q}}_\alpha$.

Definition 9.31. Let $\mathbb{P}$ and $\mathbb{Q}$ be partial orders and let $e : \mathbb{P} \to \mathbb{Q}$ be an embedding. I.e., let e be 1-1 and such that for all $p_0, p_1 \in \mathbb{P}$, $p_0 \leq p_1$ iff $e(p_0) \leq e(p_1)$. Then e is a *complete embedding* if it preserves $\perp$ and for all $q \in \mathbb{Q}$ there is $p \in \mathbb{P}$ such that whenever $r \in \mathbb{P}$ is an extension of p, then r is compatible with q.

Lemma 9.32. *Let $e : \mathbb{P} \to \mathbb{Q}$ be an embedding of partial orders in the ground model M. Then e is a complete embedding iff for every $\mathbb{Q}$-generic filter F over M, $G = e^{-1}[F]$ is $\mathbb{P}$-generic over M.*

If $e : \mathbb{P} \to \mathbb{Q}$ is a complete embedding, then there is a $\mathbb{P}$-name $\mathbb{Q} : \mathbb{P}$ for a forcing notion such that forcing with $\mathbb{Q}$ is equivalent to forcing with $\mathbb{P} * (\mathbb{Q} : \mathbb{P})$.

Lemma 9.33. *Let $((\mathbb{P}_\alpha)_{\alpha \leq \delta}, (\dot{\mathbb{Q}}_\beta)_{\beta < \delta})$ be a finite support iteration and let $\beta < \delta$. For every $p \in \mathbb{P}_\beta$ let $e_\beta(p) \in \mathbb{P}_\delta$ be such that $e_\beta(p) \restriction \beta = p$ and for all $\alpha < \delta$ with $\alpha \geq \beta$, $e_\beta(p)(\alpha) = \dot{1}_{\mathbb{Q}_\alpha}$. Then e is a complete embedding.*

Now let G be $\mathbb{P}_\delta$ generic over the ground model M. Then for every $\beta < \delta$, $G \restriction \beta = e_\beta^{-1}[G]$ is $\mathbb{P}_\beta$-generic over M. Let $\alpha < \delta$. Then $\mathbb{P}_{\alpha+1} = \mathbb{P}_\alpha * \dot{\mathbb{Q}}_\alpha$ and hence there is a $\dot{\mathbb{Q}}_\alpha$-generic filter G_α over $M[G \restriction \alpha]$ such that $G \restriction (\alpha + 1) = (G \restriction \alpha) * G_\alpha$.

Lemma 9.34. *Let $((\mathbb{P}_\alpha)_{\alpha \leq \delta}, (\dot{\mathbb{Q}}_\beta)_{\beta < \delta})$ be a finite support iteration. If for each $\alpha < \delta$,*
$$\mathbb{P}_\alpha \Vdash \text{``}\dot{\mathbb{Q}}_\alpha \text{ is c.c.c.''},$$
then $\mathbb{P}_\delta$ is c.c.c. In short, finite support iterations of c.c.c. forcings are c.c.c.

Theorem 9.35. *Martin's Axiom is consistent with the negation of CH.*

Proof. Let M be a countable transitive model of GCH. In M we construct an iteration
$$((\mathbb{P}_\alpha)_{\alpha \leq \aleph_2}, (\dot{\mathbb{Q}}_\beta)_{\beta < \aleph_2})$$
of c.c.c. forcing notions such that for all $\alpha < \aleph_2$, $\dot{\mathbb{Q}}_\alpha$ is forced to be of size $\aleph_1$ and for every $\mathbb{P}_{\aleph_2}$-generic filter G over M and every c.c.c. partial order $\mathbb{Q}$ of size $\aleph_1$ in

$M[G]$ there are cofinally many $\alpha < \aleph_2$ such that $(\dot{\mathbb{Q}}_\alpha)_{G\restriction\alpha} \cong \mathbb{Q}$. It can be shown that $M[G] \models \mathrm{MA} + 2^{\aleph_0} = \aleph_2$. $\qquad\square$

References

[1] T. Jech, *Set Theory*, Academic Press (1978)
[2] K. Kunen, *Set Theory, An Introduction to Independence Proofs*, North Holland (1980)

Department of Mathematics, Boise State University, 1910 University Drive, Boise, ID 83725-1555

E-mail address: geschke@math.boisestate.edu