Preprint, Institute of Mathematics, AS CR, Prague. 2007-12-20

A quick guide to independence results in set theory

Radek Honzík[1]

Supported by grant GA ČR no. 401/03/H047

Introduction. Many people feel a bit suspicious as regards modern set theory since many of its results are stated in terms of consistency. Arguably, this might mean that set theory doesn't tell us what is true, or at least provable, but rather what is *not provable*. Be it as it may, if one wants to have basic understanding of modern set theory, he or she must have some familiarity with techniques used to obtain consistency results. This article should provide introduction to these techniques without assuming special traning in set theory.

Consistency results are an integral part of set theory at least for the following two reasons. First, many questions about sets do not seem to have an intuitively acceptable unique solution; this suggests that the axioms (or basic "truths") which we accept today are not rich enough. Consistency results can thus be construed as an improvement of our understanding of sets in general. Examples of such questions include the *Axiom of Choice, AC* or the *Continuum Hypothesis, CH* which we discuss in some detail in this article. Second, there exists in set theory a very general technique for showing consistency results. Other areas of mathematics are not so "lucky" and hence – with some degree of exaggeration – we could claim that consistency results do not occur so frequently in other areas of mathematics because people do not know how to obtain such results (this in particular true of arithmetics). This technique for obtaining consistency results in set theory is called *forcing*, and it is the main focus of this article.

1 Naive set theory

Majority of introductory books into the set theory, such as [Kun80] and [Bal00], start with the list of axioms, sometimes with motivation for each axiom. But even with motivations this may seem unattractive to an interested reader because he or she may (justly) argue that introductions to arithmetics or analysis don't proceed in this formal fashion. It may support the (mistaken) conviction that set theory is utterly artificial since it lacks a true background from which it could draw its intuitions.

[1]radek.honzik@dobris.net, radek@logic.univie.ac.at. This version November 24, 2007

Yielding some ground to these objections, we will do set theory in this section without formal restrictions, enjoying the "naive" approach. It will become increasingly obvious, however, that its strategy is not viable and will have to be changed.

1.1 Basic truths

Though not formulated as axioms in some formal system, we will still have to say what we consider true of sets. The very fact that we have to do this shows that we are less certain with respect to sets then, for instance, with respect to natural numbers. There will be no attempt to give some "minimal" list (neither "ultimate"), nor the most economical one.

Also – although it may be superfluous and redundant for most of the readers – it is prudent to clear one possible cause of misunderstanding just at the beginning. It is fairly common to think that there are two kinds of objects in set theory: *sets* and *elements*, and that an element is in some sense basic and connot contain other elements (the notorious example of a bag of apples). This picture is of course wrong. In fact, there is only one kind of objects, namely *sets*; "to be an element of" is a *binary relation* between two sets, and this fact is denoted as $x \in y$, where x, y are sets.

For better orientation we may divide the basic truths into two groups: (i) *structural properties*, and (ii) *algebraic properties.*

Definition 1.1 *The* basic truths *are the following statements.*

(i) Structural properties.

– We completely ignore the question *what* sets are, both in the metaphysical and physical sense.

– *Extensionality.* Two sets will be identical iff[2] they have the same elements; i.e. we disregard any intensional properties of the elements.

– *Infinity.* The natural numbers, taken all together, are a set. In set theory, this set is customarily denoted as ω.

(ii) Algebraic properties.

– *Pairing.* For any two sets x, y there is another set $\{x, y\}$ that contains exactly the sets x, y.

[2] "Iff" is shorthand for "in and only if".

– *Union.* For any set x there is another set $\bigcup x$ that contains all elements of all the elements of x (i.e. y is in $\bigcup x$ iff there is another set z in x, and y is in z).

Comment. This operation has an obvious connection with the $\cup$ operation known from the basic (school-taught) set theory:

$$\bigcup\{x, y\} = x \cup y.$$

$\bigcup$ is obviously more general – unlike the $\cup$ operation which joins elements from *two* sets, $\bigcup$ can join the elements of arbitrarily many sets (their number is determined by the size of x in $\bigcup x$).

– *Power set.* For any set x there is another set $\mathscr{P}(x)$ which contains exactly all the subsets of x.

– *Closure under arbitrary set-operations.* For any operation F from sets to sets, the image of F from a set x is also a set, i.e. $F''x = \{y \mid \exists q \in x \text{ such that } y = F(q)\}$ for a set x is a set.

Comment. In formulating this property we have admittedly crossed the line of what is intuitively true. But a weakening of the above property is intuitive: if P is a property and x a set then there is a set y which contains exactly the elements of x satisfying property P. The stronger form is however necessary even for the most elementary proofs.[3]

The reader may wonder what about other properties which are widely known, such as *axiom of choice*, *continuum hypothesis* and other. Well these are not intuitively true (or false) so we should try to show them true or false – but before we do this, we first have to know more about sets, based on the basic properties we have just given.

We close this paragraph with a technical note. The above assumptions postulate what objects are sets. For instance if x is a set, then $\mathscr{P}(x)$ is a set. But what about $X = \{x \mid x \notin x\}$? We know from the Russell's paradox, that X must not be a set, or else our system is inconsistent.[4] The crucial point here is how new sets are formed – it is tempting, and this is what Frege, who much to his misfortune introduced the so called Russell's paradox into his system for arithmetics, effectively did, to be as general as possible: a set is an arbitrary collection of objects satisfying some property. If, however,

[3] It is necessary for definition of a function by recursion. Recursion is for instance indispensable in the proof that axiom of choice is equivalent to the claim that all sets can be wellordered. For more details about recursion, see Fact 2.1.

[4] Denote $X = \{x \mid x \notin x\}$. But then $X \in X$ implies $X \notin X$, and $X \notin X$ implies $X \in X$, so we have a contradiction.

we accept this general rule to form new sets, or technically speaking this form of *axiom of comprehension*, we get the above contradiction – $x \notin x$ is certainly a property and X should accordingly be a set. So we must be more restrictive and include some safeguards in our system. It turns out that the statements under the heading "Closure under arbitrary set-operations" provide these safeguards. In effect, they allow a new set to be created only from a set which already exists. For instance if x is a set, then $\{y \in x \mid y \notin y\}$ is a set; the reader may verify for himself or herself that this time we don't get a contradiction.

To complicate things a little, the object $X = \{x \mid x \notin x\}$ – which we have just now excluded from our universe of sets – is nonetheless too "intuitive" to be banned altogether. In fact, under the axiom of foundation (see Definition 2.2), the object X contains all sets which exist, i.e. $X = \{x \mid x = x\}$. We have agreed that this is not a set, but we still want to "refer" to it for practical purposes. To cut long story short, we will distinguish two kinds of objects: *sets* and *classes*. The latter objects may be too big to be sets and we will have to treat them with some caution.[5] Some classes can also be sets, but those which are not sets are called *proper classes*. Canonical examples of the proper classes are the class $X = \{x \mid x = x\}$, which is customarily denoted V, or the proper class of ordinal numbers, On, to be defined below. For more rigorous treatment, see discussion after Definition 2.2.

1.2 The notion of "size" or "magnitude"

There are many things which are true about sets, but it seems most natural to concentrate on the notion of "size" since set theory is, after all, about "big" sets.

The most obvious question is if we have "more" infinity than just the set of natural numbers. There can be several approaches which clarify the idea of "more infinity"; with some generalization, we can distinguish two main types: comparison via the 1-1 functions or via the types of wellordering.[6]

The first notion is in some sense stronger (but also coarser, as the reader shall see further on) so we will take it up first.

We say that x is smaller than y if there is a 1-1 function from x to y.[7] We shall denote this relation as $|x| \leq |y|$. If $|x| \leq |y|$, but $|y| \not\leq |x|$, we write $|x| < |y|$ and say that x is strictly smaller than y. Note that this definition

[5] This compares nicely with the situation in arithmetics: the set of all natural numbers is certainly not a natural number, but we still (indirectly) refer to it when we claim that something is true about all natural numbers.

[6] A function f is 1-1 if no two distinct x_1, x_2 in the domain of f have the same image, i.e. $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$.

[7] To avoid confusion, this function is itself a *set*, construed as a set of ordered pairs, and must be first shown to exist.

is reasonable in the sense that the usual "sizes" of natural numbers satisfy this property, for instance $|n| < |n+1|$ is true for all n.[8]

Theorem 1.2 (Cantor) *For any set x,*

$$|x| < |\mathscr{P}(x)|.$$

In particular, if ω denotes the set of all natural numbers,

$$|\omega| < |\mathscr{P}(\omega)|,$$

i.e. we have more infinity than just natural numbers.

Proof. We only show that $|\omega| < |\mathscr{P}(\omega)|$ since the generalization to an arbitrary x is immediate. We first show that (i) $|\omega| \leq |\mathscr{P}(\omega)|$, and then we show (ii) $\mathscr{P}(\omega) \not\leq |\omega|$; this implies that $|\omega| < |\mathscr{P}(\omega)|$ as required. (i) is obvious: define g to map $n \in \omega$ to $\{n\} \in \mathscr{P}(\omega)$. To prove (ii) we argue by contradiction. For contradiction suppose there is 1-1 function f from $\mathscr{P}(\omega)$ into ω. Consider the set

$$A = \{n \in \omega \,|\, n \notin f^{-1}(n)\},$$

for all n in the range of f. As A is a subset of ω, A is in the domain of f; let a denote the image of A under f, i.e. $f(A) = a$. Then there are two possibilities: (a) $a \in A$, but then by definition of A, $a \notin f^{-1}(a) = A$, contradiction; (b) $a \notin A$, but then $a \notin f^{-1}(a)$, and thus satisfies the property defining A, hence $a \in A$, contradiction. As both possibilities lead to contradiction, we have proved that $|\mathscr{P}(\omega)| \not\leq |\omega|$. $\square$

It may be added that the structure of the proof is a "positive incorporation" of the Russell paradox into the set theory. See discussion after Definition 1.1.

At first glance, the set $\mathscr{P}(\omega)$ may seem somewhat artificial. We show that practically for all purposes, it can be identified with the real numbers, $\mathbb{R}$. We shall only show that $\mathscr{P}(\omega)$ has the same size as $\mathbb{R}$, but the analogy can be taken much further.[9]

Lemma 1.3 $|\mathscr{P}(\omega)| = |\mathbb{R}|$*, i.e. there is 1-1 function from all subsets of natural numbers onto the set of all real numbers.*

[8] Here we use the standard set-theoretical usage which identifies a natural numbers with the set of its predecessors: $n = \{0, \ldots, n-1\}$; in particular n has n elements.

[9] For those familiar with topology, in set theory $\mathbb{R}$ is customarily identified with the product topology on 2^ω (the so called *Cantor discontinuum*), or on ω^ω (the so called *Baire space*).

Corollary 1.4 *There are more real numbers than natural numbers.*

Sketch of proof. Though it is possible to construct directly a function f which is 1-1 and onto, we will be more lenient and demand only that $|\mathscr{P}(\omega)| \leq |\mathbb{R}|$ and $|\mathbb{R}| \leq |\mathscr{P}(\omega)|$.[10] First notice that the size of all real numbers is the same as the size of the unit interval $(0, 1)$. Without going into details, the basic idea is to write each $r \in (0, 1)$ in its (perhaps infinite) binary expansion (i.e. using only the numbers 0 and 1) and view this expansion as a characteristic function of a subset of the natural numbers (i.e. if there is 1 at place n of the binary expansion, then think of n as being a member of the corresponding set; if there is 0 at place n, then n is not in the set).[11] □

The other type of infinity – based on wellorderings – is in some sense finer than the comparisons utilizing 1-1 embeddings.

Definition 1.5 *A binary relation $<$ is a* partial ordering *on A if the following conditions hold:*[12]

(i) $<$ is irreflexive, i.e. for all a in A, $a \not< a$;
(ii) $<$ is transitive, i.e. for all $a, b, c \in A$, $a < b$ and $b < c$ implies $a < c$.

Notice that *partial* ordering doesn't demand that all members of A are comparable, i.e. it doesn't have to be true that for all $a, b \in A$, either $a < b$ holds, or else $b < a$. If it does hold that for all $a, b \in A$, either $a < b$ holds, or else $b < a$, we call such ordering *linear*.

Definition 1.6 *We say that A is* wellordered *by $<$ if $<$ is a partial ordering on A and for every $X \subseteq A$ the ordering $<$ restricted to X has a least element.*

Note that this definition in particular implies that $<$ on A is linear. The most prominent example of a wellordered set is $\mathbb{N}$, or in set-theoretical notation, ω, i.e. the set of natural numbers (if $X \subseteq \omega$, pick any $x \in X$; then $\{y \leq x \,|\, y \in X\}$ is finite and certainly has a least element). Also note that the whole numbers, or integers, denoted $\mathbb{Z}$, are *not* wellordered – the set of negative numbers doesn't have a least element. Disregarding niceties, the assumptions given in Definition 1.1 allow us to prove that there is a set that

[10] It is a theorem in set theory, the so called *Cantor-Bernstein* theorem, which claims that we are perfectly entitled to do this, i.e. that $|A| \leq |B|$ and $|B| \leq |A|$ already implies $|A| = |B|$.

[11] The more careful argument has to take into consideration that for instance the number $0,00\bar{1}$ is the same as $0,01\bar{0}$ though the corresponding sets are different; a hint to the reader: when constructing a function from $\mathscr{P}(\omega)$ into $(0, 1)$, think of $(0, 1)$ as a disjoint union of $(0, 1/2)$ and $(1/2, 1)$ and map the set $0,00\bar{1}$ into one half and the set $0,01\bar{0}$ into the other.

[12] We must emphasize that $<$ is in fact a set consisting of ordered pairs; we write $x < y$ to denote $\langle x, y\rangle \in <$.

contains one more element than ω and the ordering $\leq$ on ω can be so extended that the new element is bigger than all elements of ω (in simple terms, take all elements of ω and put one new element after them all). Let us denote this set suggestively as $\omega + 1$, and the new element ω.[13]

We now show the simple observation that using the notion of infinity based on 1-1 functions, ω has the same size as $\omega + 1$, but with respect to the wellordering $\leq$, the set $\omega + 1$ is strictly longer (or "bigger").

Observation 1.7 $|\omega| = |\omega + 1|$, *but* $(\omega, \leq)$ *and* $(\omega + 1, \leq)$ *are not order isomorphic, i.e. there is no 1-1 function* i *from* ω *onto* $\omega + 1$ *such that* $n \leq m$ *iff* $i(n) \leq i(m)$.

Proof. For the first claim, define $i(0) = \omega$ and $i(n) = n - 1$, for $n > 0$. The second claim follows easily from the fact that whereas in ω all elements have finitely many predecessors, in $\omega + 1$, ω has infinitely many predecessors. $\square$

Note also, that there are many sets that are not identical, but still are order isomorphic (such as the set of all even numbers with the inherited ordering and the set of all natural numbers) – hence our result is not automatic.

We can iterate the above process, and obtain a sequence of ever longer sets

$$\ldots \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega \ldots,$$

where $\omega + \omega$ is intuitively a set consisting of two copies of ω put one after the other. But we needn't stop at that – writing $\omega \cdot 2$ for $\omega + \omega$, we obtain

$$\omega \cdot 2, \ldots, \omega \cdot 2 + 3, \ldots \omega^2,$$

where ω^2 is written for $\omega \cdot \omega$. But again, we may continue

$$\omega^2, \ldots, \omega^2 \cdot 3 + \omega \cdot 15, \ldots \omega^3, \ldots \omega^\omega.$$

And there is no need stop here, either.

But what is perhaps surprising is that it is relatively simple to show that all these sets are still *countable*, i.e. there is a 1-1 function mapping them onto ω. The question presents itself whether we can reach something uncountable by this procedure.

1.3 All is about wellorderings . . .

Yes, we can; and this fact follows from Theorem 1.2 and the fact that $\mathscr{P}(\omega)$ "should" be wellorderable.[14] This "should" deserves further clarification.

[13] In fact, under the formal definition, $\omega + 1$ is identified with $\omega \cup \{\omega\}$, the ordering $\leq$ being the $\in$ relation.

[14] As a matter of fact, this assumption about wellordering of $\mathscr{P}(\omega)$ is not necessary; but it simplifies the argument and also motivates the notion of a wellordering.

Given a set x we could wonder whether there is a relation $<$ such that x is wellordered by $<$. General agreement is that such $<$ should exist; the reasons for this agreement range from pragmatic issues (wellorderings add a powerful structuring to the universe and help to prove various theorems; see the discussion after Fact 1.11), to aesthetic considerations (some consider a universe without such wellordering as badly organized).

Without inquiring – at least for the time being – whether the existence of such wellorderings already follows from the other basic "truths" we have accepted earlier, we know add this principle into our stock of basic truths (it fits into the group (i) *Structural properties*). To be more specific, we now consider the statements WO and AC given below as true. It must be conceded, however, that the truth of WO and AC is less evident than of those given in Definition 1.1.

Definition 1.8 The wellordering principle, WO, *is the following statement: for any set x there exists a relation $<$ with domain x such that $(x, <)$ is a wellordered set.*

One of the earliest theorems in set theory, the one which has given rise to first axiomatization, see [Zer04], is that WO is equivalent to famous AC, Axiom of Choice.

Definition 1.9 The axiom of choice, AC, *is the following statement: for any set x there is a function f with domain consisting of all non-empty elements of x such that if $y \in x$ and $y \neq \emptyset$, then $f(y) \in y$. Such f is sometimes called a* choice function.

In this abstract setting, AC doesn't look much appealing. However, it is known that many theorems in the usual mathematics are not provable without some form of AC; we will list just few of them:

(i) Every vector space has a basis;
(ii) Every field has a unique algebraic closure;
(iii) The Hahn-Banach Extension Theorem;
(iv) Tikhonov's Product Theorem for compact spaces.

Theorem 1.10 *WO is equivalent to AC.*

Sketch of proof. WO is easily seen to imply AC: given x let x' contain all elements of y, where $y \in x$; formally $x' = \bigcup x$. WO applied to x' yields some wellordering $<_{x'}$. Define $f(y)$, where $y \in x, y \neq \emptyset$, as the $<_{x'}$ least element of y.

The converse direction uses a transfinite recursion, which we have not defined rigorously.[15] Intuitively, apply AC to obtain an f on $\mathscr{P}(x)$. Then

[15]See Fact 2.1.

successively build the wellordering $<_x$ by choosing as the next element in $<_x$ the value of f applied to the subset of x which has not yet been included in the domain of $<_x$. □

1.4 Cardinals vs. ordinals

The most intriguing property of set theory is its ability to unify seemingly diverse concepts. Above, we have introduced two different concepts of size. We now show that we may identify the sizes obtained via the 1-1 functions with some of the wellordered sets. The basic property of the wellordered sets is captured in the following result we state without a proof.[16]

Fact 1.11 *Suppose* $(A, \leq_A)$ *and* $(B, \leq_B)$ *are two wellordered sets. Then there are three possibilities,*

(i) $(A, \leq_A)$ *and* $(B, \leq_B)$ *are order isomorphic;*
(ii) $(A, \leq_A)$ *can be embedded into* $(B, \leq_B)$ *as a proper initial segment; or*
(iii) $(B, \leq_B)$ *can be embedded into* $(A, \leq_A)$ *as a proper initial segment.*

If we abstract from the concrete sets, then the above fact claims that wellordered sets can be nicely put one after the other, and that they effectively form a stick which can be used to "measure" the length of sets (endowed with some ordering). Their role in set theory is omnipresent and cannot be overstated – they are the true generalization of the natural numbers. It turns out that if we define the equivalence on wellordered sets (two sets will be equivalent iff they are order isomorphic), then in each equivalence class we can find one special set which we declare to be the "representative" of the class.[17] This representative is simplest possible in the sense that it is of the form $(X, \in)$, i.e. the ordering is given by $\in$ (i.e. the binary relation $\in$ satisfies Definition 1.5 on the domain X).

Definition 1.12 *These representatives are called* ordinals*, or* ordinal numbers.[18] *They are two types of ordinals:*

(i) Successor *ordinals; i.e. ordinals which have an immediate predecessor. For instance all natural numbers are successor ordinals, but also the set* $\omega + 1$ *– which is technically speaking identical with* $\omega \cup \{\omega\}$ *– is a successor ordinal;*

[16] The proof is straightforward, but requires some technical apparatus.

[17] This is common mathematical practice. Recall that the same happens with rational numbers: $1/2$ is considered the same number as $2/4$, $3/6\ldots$, and the representative is defined as the one with non-divisible constituents.

[18] The real definition must be more careful, and is consequently more obtuse: x is ordinal number iff it is transitive and wellordered by $\in$.

(ii) Limit *ordinals; i.e. ordinals which don't have an immediate predecessor. For instance ω, i.e. the set of all natural numbers, or $\omega + \omega$ are limit ordinals.*

Ordinal numbers, for short "ordinals", will be denoted by small Greek letters from the beginning of the alphabet ($\alpha, \beta, \gamma \ldots$). The class of all ordinal numbers will be denoted On. Some of the members of the class On were introduced – without the term "ordinal" – at the end of Section 1.2.

Now, we may apply the property of being of the same size (using the 1-1 functions) to the structure of wellordered sets. We have seen that for instance ω and $\omega+1$ are *different* ordinal numbers, but modulo 1-1 functions are equivalent (see Observation 1.7). Formally,

Definition 1.13 *An ordinal number κ is called a* cardinal number *if there is no 1-1 function f and an ordinal number $\alpha < \kappa$ such that f maps 1-1 the ordinal κ onto the ordinal α.*

To draw an intuitive picture: there is a wellordered class of all ordinal numbers (we may picture it as a line), representing the types of wellordered sets (in the sense of Fact 1.11), and some ordinals on this line have the additional property that there are the least in the segment of ordinal numbers with the same size with respect to 1-1 functions.

We have seen that the cardinal numbers are very rare between the ordinal numbers: recall that $\omega + 1, \omega^2, \omega^\omega, \omega^{(\omega^\omega)}$ etc. are still countable ordinals, i.e. there is a 1-1 function mapping them onto ω. But there is some cardinal above $\omega + 1, \omega^2, \omega^\omega, \omega^{(\omega^\omega)}$, as the following corollary claims:

Corollary 1.14 *Assume AC (or, equivalently, WO) for simplicity. There is an ordinal number α such that $(\alpha, \in)$ is isomorphic to $(\mathscr{P}(\omega), <)$, where $<$ is some wellordering ensured by AC, and there is no 1-1 function from α onto ω. In other words there is a cardinal above ω.*

Proof. Due to Fact 1.11, the wellordering $(\mathscr{P}(\omega), <)$ implies that there is some ordinal $(\alpha, \in)$ order-isomorphic with $(\mathscr{P}(\omega))$.[19] The second part of the claim follows from Cantor's theorem 1.2. □

The above result easily generalizes to all cardinals by induction (for instance the size of $\mathscr{P}(\mathscr{P}(\omega))$ is clearly bigger than $\mathscr{P}(\omega)$).

[19] We do a little cheating here: we use the additional (unmentioned) fact that the totality of all ordinal numbers is a class – something bigger than any set; since $\mathscr{P}(\omega)$ is certainly a set (see the statement of *power set* property in Definition 1.1), there must be some ordinal number – an element of the class of all ordinal numbers – corresponding to $(\mathscr{P}(\omega), <)$. The point is that it could conceivably happen that what corresponds to $(\mathscr{P}(\omega), <)$ is the wellordered totality of *all* ordinal numbers.

Corollary 1.15 *Assume AC (or, equivalently, WO) for simplicity. Then the class of all cardinal numbers is unbounded and continuous among the ordinal numbers; in particular there is a proper class of cardinal numbers.*

1.5 Alephs: $\aleph_\alpha$

We are now in a position to define the notion of an $\aleph$, arguably the most popularized symbol of set theory.

We will start with the following fact.

Fact 1.16 *Whenever $(X, <)$ is a proper class wellordered by $<$ with the additional property that for each $x \in X$, $\{y \in X \mid y < x\}$ is a set (not a proper class), then $(X, <)$ is isomorphic to the class of all ordinal numbers ordered by $\in$.*

Due to Fact 1.16 and Corollary 1.15, there is a function i from ordinal numbers onto the cardinal numbers which is 1-1. In other words, this function *enumerates* the cardinal numbers in the sense that $i(\alpha)$ is the αth cardinal number. Since i is identity on ω (i.e. $i(n) = n$ for all $n \in \omega$), it is customary to start the enumeration of the cardinals with ω, the least infinite cardinal. The function which enumerates the infinite cardinals is denoted $\aleph$, where for notational reasons $\aleph_\alpha$ is written for $\aleph(\alpha)$. For illustration, $\aleph_0 = \omega$, $\aleph_1 =$ the first cardinal greater then ω, and so on.[20]

Due to Fact 1.16, the enumeration by $\aleph$ is defined on all ordinal numbers – for any ordinal α there is the αth cardinal number, denoted $\aleph_\alpha$. By way of illustration, the following are cardinal numbers:

$$\aleph_0, \aleph_1, \cdots, \aleph_\omega = \aleph_{\aleph_0}, \cdots, \aleph_{\aleph_1} = \aleph_{\omega_1}, \cdots .$$

Note that we can now give a more precise meaning to the notation $|x| \leq |y|$ which we have introduced earlier. Under AC, every x can be wellordered, and so the size of x can be defined as the unique cardinal $\aleph_\alpha$ such that x can be mapped 1-1 in an order-preserving fashion onto $\aleph_\alpha$ (see Fact 1.11). The relation $|x| \leq |y|$ thus translates to saying that the cardinal corresponding to x is less than or equal to the cardinal corresponding to y.

Though the statement of Fact 1.16 may seem very innocuous and plausible at the first glance it should be remembered that it implies that the number of ordinal numbers and the number of cardinal numbers is the same; so even

[20]To avoid future cause of confusion, it is customary in set theory to use two kinds of notation for alephs: $\aleph_\alpha$, vs. ω_α. Strictly speaking, it is always true for all $\alpha \in$ On that $\aleph_\alpha = \omega_\alpha$; however, the notation ω_α is used in the situations where we look at cardinal number $\aleph_\alpha$ in terms of its being an ordinal. A typical example of this convention is the notation $\aleph_{\omega_1}$, where we stress the point that we talk about a cardinality which is indexed by the first uncountable cardinal $\aleph_1 = \omega_1$.

if there are great "gaps" between cardinal numbers, there is still the same number of them as of all ordinal numbers. This is paradigmatic example of results which clearly run contrary to intuition formed when dealing with finite objects.

1.6 How big is $\mathbb{R}$

The natural question now is what is the place of $\mathbb{R}$ on the $\aleph_\alpha$ scale. Theorem 1.2 and Lemma 1.3 together with AC imply that $\aleph_1 \leq |\mathbb{R}|$, but can we say something more? Surprisingly, even if the question may seem very trivial, Cantor and other set-theoreticians worked for more than 30 years and obtained only partial results.[21]

Definition 1.17 *Continuum hypothesis, CH, claims that the size of* $\mathbb{R}$*, or* continuum*, is the least possible, i.e.* $|\mathbb{R}| = \aleph_1$.

Now we – as the set-theoreticians in the early 30s – have arrived at an important crossroads – if we wish to be faithful to our "naive" set-theoretical framework (i.e. no axioms, just "truths"), then all left to us would be to keep trying to decide whether the CH is true or not. With the benefit of hindsight, we know that such efforts would be hopeless.

2 Axiomatic set theory

If there is a persistent failure to decide a given statement (such as CH in the 30s), it is reasonable to ask whether it is *in principle* possible to decide this statement. However, in the framework of our "naive" set theory – centered on truth of statements – any inquiry about the *principal* feasibility of such a task is a priory meaningless. Truth is an absolute concept, every statement is true or false, regardless of our ability to determine it.

For practical reasons we may therefore decide to replace the concept of truth by something weaker. In principle, there may be innumerable ways how to do it. In practice, this weaker concept is almost exclusively taken as that of a *proof* inside some formal calculus. In the case of set theory,

[21] The above question about the size of $\mathbb{R}$ may be reformulated as follows: does there exist an infinite set $X \subseteq \mathbb{R}$ that is neither of size ω, nor of the maximum size possible, i.e. $|\mathbb{R}|$? If there is no such set X, then indeed $|\mathbb{R}| = \aleph_1$. Cantor and others defined subsets X of $\mathbb{R}$ of ever increasing complexity and always succeeded in proving that it is either of size ω, or has the maximum size. For instance all closed subsets of $\mathbb{R}$ have this property. But they never succeeded in showing this for all subsets X.

this formal calculus is almost universally based on the first-order predicate calculus.[22]

The replacement of the notion of "truth" by the concept of "proof" has some benefits, as well as deficiencies. By restricting the domain of our inquiries to proofs[23] we are suddenly able to show that a given statement is not decidable inside our system, i.e. is not provable from the chosen assumptions; on the other hand we implicitly exclude some truths from our formal system.[24]

In devising the formal system, i.e. deciding upon the axioms we choose, we obviously aim at capturing as big a portion of the interesting and intuitively true statements as possible. Accordingly, if we show that a given interesting statement φ is independent of our system, i.e. is not provable nor refutable, we will construe this positively as an opportunity to increase our understanding of the given area of mathematics.We will give examples of such statements in set theory in the next paragraphs. A famous example from another part of mathematics is the 5th Euclid postulate – the realization that it is independent of the first four postulates opened doors to non-standard geometry and hence better understanding of the subject.

2.1 Zermelo-Fraenkel axiomatization

The following list of axioms (formulated in the 1st order predicate calculus) is now considered as standard.

Before we give the list of axioms, we will formulate in more detail the concept of *recursion*, or equivalently *induction*. We have mentioned recursion in passing above, but from this spot on, this concept deserves more rigorous treatment. We shall not give a formal proof of the properties of the construction, but rather explain what is going on.

Fact 2.1 *For each class function G from V to V there exists a unique class function F such that for all ordinal numbers α,*

$$F(\alpha) = G(F \restriction \alpha),$$

where $F \restriction \alpha$ is the function F restricted to the domain α.

[22] Arguably, the main reason for the adoption of the first order predicate calculus seems to be the ease of use of the calculus, in particular the completeness theorem and Löwenheim-Skolem theorems; in other systems some of these benefits are always lost.

[23] For obvious reasons, the formal framework is always designed so that what is provable is also true, so that we may fail to capture every true statement, but we only capture true statements and no false ones.

[24] In case of reasonable theories, such as set theory or even arithmetics, it can be shown that we always exclude some truths; this is of course the consequence of Gödel's incompleteness theorem.

Comment. The transfinite recursion given in Fact 2.1 above is a simple generalization of the classical definition by recursion along the natural numbers – the function G can be viewed as procedure which will calculate the value of F at ordinal α based on the values F takes on $\beta < \alpha$ (we may see G as the simpler function of the two defining the more complex function F).[25] The recursion along On must be defined at limit ordinals as well, but the principle is the same.

Now we may give the list of axioms.

Definition 2.2 *The* Zermelo-Fraenkel, ZF *set theory is comprised of the following axioms; cf. with the list in Definition 1.1.*[26]

- *Extensionality.*

  $\forall x, y\, [x = y \leftrightarrow (\forall q\, q \in x \leftrightarrow q \in y)]$.

- *Pairing.*

  $\forall x, y\, \exists z\, [\forall q\, (q \in z \leftrightarrow q = x \vee q = y)]$

  Comment. We shall write $z = \{x, y\}$.

- *Union.*

  $\forall x\, \exists z\, [\forall q\, (q \in z \leftrightarrow \exists y\, y \in x \wedge q \in y)]$

  Comment. We shall write $z = \bigcup x$.

- *Powerset.*

  $\forall x\, \exists z\, [\forall q\, (q \in z \leftrightarrow q \subseteq x)]$

  Comment. The symbol $q \subseteq x$ is shorthand for $\forall q'\, (q' \in q \rightarrow q' \in x)$. We shall write $z = \mathscr{P}(x)$.

- *Schema of replacement; closure under arbitrary set-operations.*

  We say that a formula $\varphi(x, y)$ determines a function if

  $\forall x, y, y'\, (\varphi(x, y) \wedge \varphi(x, y') \rightarrow y = y')$

  then the following is taken as an axiom:

[25] Consider the following easy example: $F(0) = 1$ and $F(n+1) = 2^{F(n)}$. The existence of such a function follows from Fact 2.1. Note that we only need to know the value of $F(n)$ to calculate $F(n+1)$; and hence the relevant G for this F is a function which maps n to 2^n. (This particular G is in fact obtained by recursion itself: this time the relevant G' takes n to $2n$.)

[26] For technical reasons the listed order of the axioms is different than in Definition 1.1; for instance, it is convenient to have the pairing function defined before the axiom of infinity is stated. For more detailed and rigorous treatment of the axioms, see [Bal00], [Kun80], and [Jec03].

$\varphi(x, y)$ determines a function $\rightarrow [\forall x\, \exists z\, [\forall q\, (q \in z \leftrightarrow \exists y \in x\, \varphi(y, q))]]$

Comment. The rather awkward formulation can be translated as follows: given some arbitrary function φ which doesn't even have to be a set (note it is given by a formula), the image of any *set* x under this function φ is also a *set* (z in the axiom above). Also note that there is such axiom for any formula φ; since there is infinitely many of such formulas, the axiomatization ZF is infinite.

– *Infinity.*

  $\exists y\, [\emptyset \in y \wedge (\forall q\, (q \in y \rightarrow q \cup \{q\} \in y))]$

  Comment. At this stage it would be technically cumbersome to define first the notion of natural numbers and then claim that there is the set of all natural numbers (though it is perfectly possible to do so). So for simplicity, we just claim that there is a set with a specific property, i.e. being *inductive* (for $q \in y$, $q \cup \{q\} \in y$); there may be more such sets, we just claim that there exists at least one. Once we define the notion of a natural number, the existence of an inductive set will imply the existence of the set of all natural numbers.

– *Foundation.*

  Assume we have build ordinal numbers and showed Fact 2.1 based on the axioms above. The axiom of foundation claims the following:[27]

  Define class WF by recursion along the ordinal numbers On as follows:

$$
\begin{aligned}
WF_0 &= \emptyset \\
WF_{\alpha+1} &= \mathscr{P}(WF_\alpha) \\
WF_\lambda &= \textstyle\bigcup_{\alpha<\lambda} WF_\alpha, \text{ for } \lambda \text{ limit ordinal} \\
WF &= \textstyle\bigcup_{\alpha\in \mathrm{On}} WF_\alpha
\end{aligned}
$$

  The axiom of foundation claims that every x in the universe V is present in some level WF_α, i.e. $V = WF$.

  Comment. This axiom was not included in the list of truths in Definition 1.1 because its intuitive underpinning is not so obvious. Amongst its consequences is for instance the exclusion from the set-theoretic universe V of the sets x such that $x \in x$. It can be argued that the existence of sets with the property $x \in x$ is simply of no consequence for the usual arguments in set theory. Last but not least, the foundation axiom adds a very convenient structuring into the universe and consequently simplifies some arguments.

[27] Axiom of foundation can also be stated directly without using ordinal numbers.

Remark. We owe the reader some rigorous comments as regards the notion of a *class*. If $\varphi(x, \vec{p})$ is a first order formula with parameters $\vec{p}$, then the collection $\{x \mid \varphi(x, \vec{p})\}$ is a class; we may denote this class by some letter, for instance P, and use the notation $x \in P$. But we need to remember that $x \in P$ is only a shorthand for $\varphi(x, \vec{p})$. Recalling the case of the class $X = \{x \mid x \notin x\}$, we now see that the expression $X \in X$ is meaningless since it would mean substitution of a formula for a set variable. Also note that some classes are sets;[28] classes which are not sets are called *proper classes*.

For the time being, we consider ZF as the complete list of assumptions which we consider true of sets. By Gödel theorem we cannot hope that ZF decides every statement in set theory, but we may still cherish hopes that it decides all interesting statements we might consider. We already have two candidates to decide: the Axiom of Choice (AC) and the Continuum Hypothesis (CH). In the next paragraph, we will introduce a set-theoretical technique known as *forcing* powerful enough to answer the question of decidability not only for AC or CH but for virtually any set-theoretical statement.

For the sake of completeness we shall give the exact formulation of AC, WO and CH in the first order calculus.

Definition 2.3 *The following is the reformulation of AC, WO, CH in the first-order predicate calculus.*

(i) Axiom of Choice is the following formula:

$$\forall x \, \exists f \, \forall y [(y \in x \wedge y \neq \emptyset) \rightarrow y \in \mathrm{dom}(f) \wedge f(y) \in y],$$

and in view of Theorem 1.10, this is equivalent to the following statement in item (ii):

(ii) WO, the wellordering principle, is the following formula:

$$\forall x \, \exists < \; [(\forall a, b, c \in x \; a \not< a \wedge (a < b \wedge b < c) \rightarrow a < c) \wedge (\forall y \subseteq x \, \exists x_0 \in y \, \forall z \in y \, (z = x_0 \vee x_0 < z))]$$

(iii) Continuum Hypothesis is the following formula (where we write $2^{\aleph_0}$ for the size of $\mathscr{P}(\omega)$):

$$2^{\aleph_0} = \aleph_1.$$

[28]If x is a set, then $P = \{q \mid q \in x\}$ is a class in the sense of the above comment and is equal to x, so it denotes a set.

3 Independence

In the previous paragraph, we have promised to inquire whether the statements AC and CH are decidable in ZF or not. The question of decidability is obviously composed of two parts: (i) whether AC and CH are consistent with respect to ZF, and (ii) whether ¬AC and ¬CH are consistent with respect to ZF. Formally speaking, a statement φ is consistent with respect to ZF if

$$ZF \nvdash \neg\varphi,$$

i.e. there is no proof of the negation of the statement derivable from the axioms of ZF.[29]

Now, it is generally easier to show that some object exists, rather than verifying that no object from the infinitely many possibilities satisfies some property (for instance, being a proof of a statement). To transform our task to this more convenient form, we take advantage of the following basic equality between syntactical and semantical side in the predicate calculus:

$$ZF \nvdash \neg\varphi \Leftrightarrow \text{ exists a model } M \models ZF + \varphi.$$

From now on, then, to show that a statement φ is consistent amounts to finding a model for ZF + φ.[30] Note however that since we can find no model for the theory ZF due to Gödel theorem (unless we use something stronger than a set theory), we will technically speaking assume the existence of a model for ZF and from this model we shall derive a model for ZF + φ; this is known as *relative consistency*.

3.1 Transitive structures

All structures, or models, we will consider will be of the form $(M, \in)$ where $M \subseteq V$ is a class. In particular, the binary relation "to be an element of" will always be realized over the domain M by the predicate $\in$ (and the same goes for $=$). As is common in set theory, we "translate" the provability relation $ZF \vdash \varphi^M$ into a model-theoretic language and say that φ holds in M.[31]

[29]The meaningfulness of the following discussion of course presupposes that ZF itself is consistent, i.e. that it does not prove a contradiction; again due to Gödel, this time his second theorem, we cannot show that ZF is consistent; rather, we decide to take the consistency of ZF on belief.

[30]We need to excercise some care as regards the exact meaning of the word "model"; see discussion at the beginning of Section 3.1 for more information.

[31]φ^M is obtained from φ by restricting all quantifiers to M: $\exists x$ becomes $\exists x \in M$ and similarly for $\forall$. If M is a set, then $ZF \vdash \varphi^M$ is equivalent to $ZF \vdash (M \models \overline{\varphi})$, where $\overline{\varphi}$ is a formal translation of the metamathematical formula φ. If M is a proper class, then the relation $\models$ may not be definable, and so the notation $ZF \vdash \varphi^M$ is preferable.

Definition 3.1 *We say that a class X is* transitive *if for all $x \in X$ we have $x \subseteq X$, or in other words if $y \in x \in X$, then also $y \in X$.*

All models we will consider will have a transitive domain. We might even say, with a degree of exaggeration, that there are no other interesting models but transitive ones. The main reason for this is that a lot of basic properties is absolute for transitive models; this is a technical term, but its intuitive import as follows. When inquiring about properties holding in a model, say $(M, \in)$, we implicitly work in the universe V (everything we do in set theory takes place in V). It is of great advantage if some properties hold in M iff they hold in V – we have some understanding of V and it can help us understand the model M. We shall give a couple of specific examples.

Since the axiom of extensionality holds in V, we may conclude that any transitive model $(M, \in)$ satisfies the axiom of extensionality:

Lemma 3.2 *Assume M is a transitive class, then $(M, \in)$ satisfies the axiom of extensionality, i.e. $ZF \vdash (extensionality)^M$.*

Proof. We need to verify the following formula for all $x, y \in M$: $x = y \leftrightarrow \forall q \in M\, (q \in x \leftrightarrow q \in y)$. The direction $(\rightarrow)$ is trivial. So let us take up the converse direction $(\leftarrow)$. Assume for contradiction, that there is $q_0 \in x$ and $q_0 \notin y$; however, because M is transitive, $q_0 \in M$, and by the assumption q_0 must be in y, contradiction. Notice however, that if M fails to be transitive, then existence of such q_0 cannot be ruled out. $\square$

As regards the absoluteness, look for instance at the notion of a function. In the set-theoretical use, a function is a set of ordered pairs, where an ordered pair $\langle x, y\rangle$ is defined as $\{\{x\}, \{x, y\}\}$. Without transitivity of M, if $f \in M$ and even $f \subseteq M$, we still cannot conclude that f is a function in M ($\langle x, y\rangle \in M$ doesn't imply that x or y is in M unless M is transitive). On the other hand if M is transitive and $f \in M$, then f is a function in V whenever f is a function in M.

Amongst the properties which are absolute for transitive models belong: the ordered pair, function, relation, ordinal numbers, the set ω, and other.

But even nicer is that some properties are *not* absolute for transitive models $(M, \in)$; indeed, we must remember why we want to construct such models in the first place. In constructing a model $(M, \in)$, we want to make sure that some desired property holds in M, a property which is generally much more difficult – or outright impossible – to verify in $(V, \in)$. If AC, for instance, were absolute, then $ZF \vdash AC^M$ is equivalent to $ZF \vdash AC$, and this would tell us nothing new. To emphasize: the whole point of constructing models is that some properties are not absolute.

In a nutshell, we have an almost optimal situation with transitive models $(M, \in)$: the basic properties are absolute – so we can "see" into the transitive models – but this absoluteness stops conveniently at properties which we need to show consistent.[32]

Importantly, being a wellordering or the concept of cardinality – i.e. concepts relevant to AC or CH – are not absolute.

3.2 Inner models

Historically, the breakthrough on the AC came at the beginning of 30's when Gödel showed that AC is consistent with respect to ZF; this result was supplemented in 1938, see [Göd38], also by a result by Gödel that CH is consistent with respect to ZF. On both occasions he used a nice transitive model $L \subseteq V$ where both AC and CH hold.

First we define a concept of an inner model.

Definition 3.3 *A transitive class model* $(M, \in)$ *is an* inner model *if it contains all ordinal numbers, i.e.* $\mathrm{On} \subseteq M$*, and satisfies axioms of ZF, i.e.* $ZF \vdash \varphi^M$ *for every axiom* φ *of ZF.*

Now we will define an inner model L which will satisfy all axioms of ZF plus AC (and a lot of other things, such as CH).

Reviewing the axiom of foundation in Definition 2.2, we see that V is constructed from an empty set $\emptyset$ by iterating two simple operations: powerset $\mathscr{P}(x)$, and union $\bigcup x$. Gödel realized that the powerset operation is perhaps to generous – for the model to satisfy the axioms of ZF, it only needs to contain the *definable* subsets present in the universe. We will shortly make it more rigorous, but the basic idea behind the construction of L is simple enough: instead of taking the whole powerset of the earlier stage of construction (as in $\mathscr{P}(WF_\alpha)$, see the axiom of foundation), we just take the definable subsets.

Definition 3.4 *A subset* y *of the set* x *is* definable *in the model* $(x, \in)$*, to be denoted* $\mathrm{Def}_x(y)$*, if there is a formula* φ *and parameters* $\vec{p}$ *in* x *such that* y *is the set of all* q *in* x *which satisfy in* $(x, \in)$ *the property* $\varphi(q, \vec{p})$*, i.e.*

$$y = \{q \in x \,|\, (x, \in) \models \varphi(q, \vec{p})\}.$$

[32] Formally, if $(M, \in)$ is any transitive structure, then all properties given by bounded formulas, i.e. Δ_0 formulas, are absolute; if $(M, \in)$ is a model of ZF, then all Δ_1^{ZF} formulas are absolute.

Definition 3.5 *The Gödel constructible universe L is defined as follows:*[33]

$$\begin{array}{rcl} L_0 & = & \emptyset \\ L_{\alpha+1} & = & \{y \subseteq L_\alpha \mid \mathrm{Def}_{L_\alpha}(y)\} \\ L_\lambda & = & \bigcup_{\alpha<\lambda} L_\alpha, \ \textit{for } \lambda \textit{ limit ordinal} \\ L & = & \bigcup_{\alpha\in\mathrm{On}} L_\alpha \end{array}$$

Note that L is referred to as a constructible universe since the amorphous character of the powerset operation in the definition of the class $V = WF$ is restricted to subsets which are *constructible* from the already existing elements using a defining property.

Lemma 3.6 *L is a transitive class.*

Proof. We will in fact show that for every ordinal α, L_α is transitive. This already implies that L is transitive: if $x \in L$, then $x \in L_\alpha$ for some α by the definition of L, and hence $x \subseteq L_\alpha \subseteq L$.

We will proceed by induction. Assume that $x \in L_\alpha$ and all L_β for $\beta < \alpha$ are transitive. If α is a limit ordinal, then $x \in L_\beta$ for some $\beta < \alpha$, and by the induction assumption $x \subseteq L_\beta \subseteq L_\alpha$. If α is a successor ordinal, say $\alpha = \beta + 1$, then by the definition of $L_{\beta+1}$, x is a subset of L_β. It follows that it is enough to show that $L_\beta \subseteq L_{\beta+1}$ because then $x \subseteq L_\beta \subseteq L_{\beta+1}$. Assume that $y \in L_\beta$, then

$$y = \{q \in L_\beta \mid L_\beta \models q \in y\} \in L_{\beta+1}$$

because by the induction assumption $y \subseteq L_\beta$. □

We will not prove all steps necessary to show that L is an inner model, i.e. that it satisfies all axioms of ZF. But we shall prove some crucial points to give the reader some flavour of what is going on.

Theorem 3.7 *L satisfies all axioms of ZF, i.e. $ZF \vdash \varphi^L$ for every axiom φ of ZF.*

Sketch of proof. We will just show that L satisfies the axiom of extensionality, infinity, and the powerset axiom.

[33] For an attentive reader we should add that the formulas used in the definition of the predicate Def_{L_α} cannot be the usual "metamathematical" formulas – a cursory review of the predicate Def_{L_α} shows that it contains the existential quantification over formulas; to be able to quantify over formulas, we must first build *formal* formulas (formal formulas are sets, and hence objects of our theory) inside our set-theoretical universe, much as the logical syntax is built inside arithmetics in the proof of Gödel incompleteness theorem.

(i) *L satisfies the axiom of extensionality.* This is a direct consequence of Lemma 3.2 and 3.6.

(ii) *L satisfies the axiom of infinity.* Since all finite sets are definable, $\omega \in L$ and consequently the axiom of infinity holds in L.

(iii) *The powerset axiom is true in L.*

We need to show the following:

$$ZF \vdash \forall x \in L \, \exists z \in L \, z = \{q \subseteq x \,|\, q \in L\}.$$

Working in V we define a function F that given a $q \subseteq x$, $q \in L$, finds the least α such that $x \in L_\alpha$. Let γ be the supremum of $\{F(q) \,|\, q \in L, q \subseteq x\}$. In L_γ we have all relevant subsets and also the set x. We now show that the powerset of x in L is a member of $L_{\gamma+1}$. To this effect we need to find a defining formula, but this is easy:

$$z = \{q \in L_\gamma \,|\, (L_\gamma, \in) \models q \subseteq x\}.$$

□

Incidentally, this proof of powerset axiom in L again shows the benefits of transitivity. For instance, we tacitly used the fact that the property "being a subset of x" is the same in L and in V. If it were different, then the enumerating function F defined in V would be useless.[34] Notice however that although the property "to be a subset" is absolute, the collection of all such subsets is *not* absolute – some subsets of x existing in V can be missing in L.

Before we give arguments for the consistency of AC and CH, we need to focus on the absoluteness of the construction of L. In fact, we need to show that L constructed inside L is again L. Reasons why we need this property are mostly technical: for instance when showing that AC holds in L we need to know that a particular construction of a wellordering of L is the same in V and L. We state this result without a proof.

Theorem 3.8 *L satisfies the sentence $V = L$, i.e. $ZF \vdash (V = L)^L$. It follows that if ZF is consistent, so $ZF + V = L$.*

[34] A reader might object that we could redefine F to some F' which would be defined on subsets of x in the sense of L. After verifying that there are only set-many of these (which is not automatic, notice that in our case we used the fact that if $q \subseteq x$ in L then $q \subseteq x$ in V, and $\mathscr{P}(x)$ in V is certainly a set), we would encounter another obstacle. Defining z at stage γ, how would we know that being a subset in L is the same as being a subset in L_γ? Here again transitivity is used.

Finally we may turn to the proof of consistency of AC and CH with respect to ZF. It should be emphasized however that the theorem leaves open the question whether in fact ZF already *proves* AC or CH (see Section 3.3).

Theorem 3.9 *L satisfies AC, i.e. $ZF \vdash (AC)^L$. This implies that if ZF is consistent, then $ZF \nvdash \neg AC$.*

Sketch of proof. We first show that $ZF \vdash (AC)^L$ implies $ZF \nvdash \neg AC$. We reason by contradiction: if $ZF \vdash \neg AC$, then as L satisfies all axioms of ZF, it also needs to satisfy all consequences of ZF – in particular $ZF \vdash (\neg AC)^L = \neg(AC)^L$; but as also $ZF \vdash (AC)^L$, and this contradicts the consistency of ZF.

We have stated above that AC is equivalent to the statement that all sets can be wellordered (WO). Instead of finding a distinct wellordering for every set, we will find a single (class) wellordering $<_L$ definable in L which wellorders all sets in L at once.

Notice that if x and y are in L and there are $\alpha < \beta$ such that x first appears in L_α and y first appears in L_β, then we can postulate that $x <_L y$ (here we use the fact that ordinals themselves are wellordered).

So it remains to define $<_L$ on the individual levels L_α (if x, y first appear at the same L_α, then we have to say which is the smaller one in the desired $<_L$). As the limit stages are just unions of the previous stages, it is enough to say how to extend $<_L$ from L_α to the next level $L_{\alpha+1}$. Let $\langle \varphi_i \,|\, i < \omega \rangle$ be some fixed enumeration of all formulas (there are only countably many of these); by induction assumption $<_L$ already wellorders L_α. Assume x, y first appear in $L_{\alpha+1}$ and x is defined by a formula φ_x using a single parameter p and y by a formula φ_y using a parameter r,[35] i.e.

$$x = \{q \in L_\alpha \,|\, L_\alpha \models \varphi_x(q, p)\} \text{ and } y = \{q \in L_\alpha \,|\, L_\alpha \models \varphi_y(q, r)\}.$$

We set $x <_L y$ iff the formula φ_x comes before the formula φ_y in the enumeration $\langle \varphi_i \,|\, i < \omega \rangle$ or if $\varphi_x = \varphi_y$, then p comes before r in the enumeration $<_L$ on L_α.

Now we are done, or rather almost done. We have constructed in V an ordering $<_L$ which wellorders L. But we need more: $ZF \vdash (<_L$ is a wellordering of the universe$)^L$, i.e. $<_L$ should be definable in L and L should think that it is indeed a wellordering. Fortunately, we have Theorem 3.8 which is enough to argue that this is really the case. □

Now we turn to CH.

[35] The case with more parameters is essentially the same.

Theorem 3.10 *L satisfies CH, i.e. ZF* $\vdash (CH)^L$. *This implies that if ZF is consistent, then ZF* $\nvdash \neg CH$.

Sketch of proof. The technical apparatus needed to show that CH holds in L goes well beyond the scope of this article. But some intuitive hints are readily available. Recall that CH says that there are as few subsets of ω as possible. The definition of $V = WF$ leaves a great leeway as regards the potential subsets of ω, not so L however. Notice that the subsets of ω in L are only constructed by using countably many formulas plus parameters from earlier levels of L. It is not all that easy so as to claim that all subsets of ω are in $L_{\omega+1}$ – this is not true, but it can be shown[36] that the levels of L where a new subset of ω can be created is bounded by $\omega_1 = \aleph_1$. Since at each L_α, $\alpha < \omega_1$, we have only countably many parameters to choose from and also have only countably many formulas to construct new sets, there can be at maximum $\aleph_1$ many of these.

The proof of CH in L easily generalizes to other cardinalities as well: for all $\alpha \in$ On,

$$ZF \vdash (2^{\aleph_\alpha} = \aleph_{\alpha+1})^L.$$

This statement is known as the *generalized continuum hypothesis*, GCH. □

As ZF + AC is consistent, we can enlarge our theory and include AC.

Definition 3.11 *ZFC will denote the theory ZF + AC.*

3.3 Forcing

By the above-mentioned results of Gödel, the consistency of AC and CH was decided in the 30s; but we have already mentioned that this result answers just half the question – the other half being the consistency of ¬AC or ¬CH. An obvious strategy would be to use the technique successful in the case of AC and CH and define a suitable inner model $M \subseteq V$ where ¬AC or ¬CH would hold. However, it turns out that we cannot do this:

Theorem 3.12 *Assume that ZF is consistent. There is no inner model M such that M satisfies* $\neg CH$ *or* $\neg AC$ *in ZF, or formally, there is no inner model M such that* $ZF \vdash (\neg CH)^M$ *or* $ZF \vdash (\neg AC)^M$.

[36]The proof to show this uses a rather remarkable property of L, called *condensation*: if $(X, \in)$ is an elementary substructure of $(L_\lambda, \in)$, where λ is a limit ordinal, then in fact $(X, \in)$ is isomorphic to some $(L_\alpha, \in)$, for $\alpha \leq \lambda$. So if $x \subseteq \omega$ is in L_γ, we take the Skolem hull inside L_γ containing x, obtaining a countable structure which is due to the condensation property isomorphic to some $(L_\alpha, \in)$ for $\alpha < \omega_1$. After making sure that $x \in L_\alpha$, we are done.

Proof. We shall use the following fact (note that this Fact implies Theorem 3.8: L is an inner model, and hence $L^L = L$ by this Fact):

Fact 3.13 *Let M be an inner model. If the definition of L is repeated*[37] *inside M instead of V – the result of this construction is denoted L^M –, then we obtain the same L as when the construction is carried out in V, i.e. $L = L^M$. In particular, this implies that $L \subseteq M$.*

Assume for contradiction that $ZF \vdash (\neg CH)^M$ for some inner model M (the case of $(AC)^M$ is analogous). By the above Fact, $ZF \vdash L \subseteq M$; but it cannot be true that $L = M$ as otherwise we would have $ZF \vdash (CH)^M$ by Theorem 3.10 and $ZF \vdash (\neg CH)^M$ by our assumption, and this is a contradiction. It follows that $ZF \vdash L \subsetneq M \subseteq V$, i.e. $ZF \vdash L \neq V$, but this contradicts Theorem 3.8. □

The impossibility to use inner models to show the consistency of ¬CH and ¬AC stalled the progress on this problem for the next 30 years. It was only in the 60s when Paul Cohen managed to develop a new technique which finally succeeded in showing the consistency of ¬CH and ¬AC, see [Coh63].

The idea of Cohen is both simple and ingenious: if we cannot use a transitive model M such that $M \subseteq V$, then what about going *outside* the universe V? In other words, we may wish to construct a transitive class M, containing all ordinal numbers and satisfying the axioms of ZF such that $M \supseteq V$. Taken literally, this idea is obviously not workable; by definition, there can be nothing outside V – after all, V is the universe containing all sets.

But set theory is very flexible in its means: though apparently contradictory, the idea of an outer model can be formalized inside ZF with surprising ease. First we realize that if we assume there is a transitive set model M of ZFC,[38] then it suffices to extend the "smaller" universe M, instead of V. In fact, what Lemma 3.12 says is that if M is a transitive model (set-like, or a proper class), then there is no M-definable transitive model $N \subseteq M$ satisfying sentences contradictory with $V = L$ – however, the situation of $M \subseteq N$, where N is defined in V, is permissible.[39]

[37] Recall that as M is an inner model, it satisfies all axioms of ZF; in particular all apparatus used in V when L is constructed is available inside M as well. But it is conceivable that the same apparatus used in V yields another result when applied in M. For instance, in both models we can form the power set of ω, but the actual sets representing the power set in M and in V can be different – depending on the subsets available in V, or in M.

[38] Due to Gödel theorem, we cannot show the existence of *any* set model of ZFC (inside ZFC), the less so of a transitive one; but much as with the existence of a model of arithmetics $\mathbb{N}$, we may decide that we believe in existence of such a model. Moreover, as will be apparent later, see page 38, the assumption of the existence of a transitive set model of ZFC is convenient, but by no means necessary for the development of the forcing.

[39] The contradiction in Lemma 3.12 centers around an existence of a hypothetical element $x \in M$ which is not constructible, i.e. $x \notin L$. But here is the snag: if M contains all

Consequently, instead of starting with V, we can start with some transitive set model of ZF, called M, extend M by some transitive $N \supseteq M$ and plan this construction in such a clever way to ensure that N also satisfies ZF.

3.3.1 Extending the universe

In the following sections, we shall briefly describe how a universe can be extended into a larger universe, also satisfying ZF. The emphasis will be on connections and background, whereas the technicalities will be suppressed. An interested reader can find an excellent rigorous treatment in [Kun80].

Recalling the discussion from the previous section, we fix a transitive countable model[40] of ZF, or ZFC.[41] We will from now on forget about the universe V, and will "live" in M instead. For instance, an ordinal number for us will be an ordinal number in M – we act as if we cannot see ordinal numbers outside M. By absoluteness properties discussed in Section 3.1, we know that ordinal numbers are absolute; it follows that ordinal numbers we see in M are the real ordinal numbers. Also, by a simple argument, the transitivity of M implies that the ordinal numbers in M form an initial segment of the ordinal numbers; in other words, there is an ordinal number o_M such that $o_M = \{\alpha \mid \alpha \in \mathrm{On}^M\}$, i.e. o_M is the least ordinal α such that $\alpha \notin M$. The ordinal o_M is called the *height* of M, and if M is countable, then $o_M < \omega_1$.

It turns out that a reasonable concept of an extension of M should preserve the ordinal height o_M, i.e. that for the desired extension $N \supseteq M$, it should hold that $o_N = o_M$. An intuitive argument for this requirement might run as follows: we need to have some control over the properties of N, and introducing new ordinal numbers into N makes this almost impossible – we need some correspondence between constructions in M and N; and since constructions in set theory heavily use iteration over the ordinal numbers, a new ordinal number in N would be literally "inaccessible" from the point of view of M.

We have so far decided that we need to extend M, a transitive countable model of ZF, into a model $N \supseteq M$, which is also to be a model of ZF. The following lemma shows that in extending the model M we must be very

---

ordinal numbers – as we assumed in Theorem 3.12, then "being constructible" and "being constructible *in the sense of* M"is indeed the same thing, i.e. $L = L^M$. But if M were a *set*, for instance, then this is no longer true: all we have is that $L^M \subseteq L$; in particular, it is perfectly possible that $L^M \subseteq M$ and $L^M \neq M$, with the offending $x \in M \setminus L^M$ existing in L!

[40] The countability conditions shall be used later, see Theorem 3.25.

[41] It is convenient to have AC in our model; by theorem 3.9 we may assume that much. In fact, very often our M will be a model of $V = L$ because this assumption greatly simplifies the cardinal arithmetics which is essential for rigorous development of forcing.

careful about the use of any "extra" information available in V, but not in M. Consequently, we cannot hope to argue recklessly in V and pick some arbitrary $x \in V \setminus M$ and build the extension N around this x. Indeed, the correct selection of such x lies at the heart of the forcing construction.

Lemma 3.14 *Assume M satisfies ZF. Let $\alpha < \omega_1$ be greater then o_M, i.e. $o_M < \alpha$. Let $(\omega, <_R)$ be isomorphic to $(\alpha, \in)$. Then for all transitive extensions $N \supseteq M$ such that $o_N = o_M$,*

if the relation $<_R$ is in N, then N is not a model of ZF.

Proof. Because $\alpha < \omega_1$, there is a function f mapping α 1-1 onto ω. If we define a binary relation $<_R$ such that $n <_R m$ iff $f^{-1}(n) \in f^{-1}(m)$, then $(\omega, <_R)$ is isomorphic to $(\alpha, \in)$; sometimes we say that $<_R$ "codes" α. Now it is a theorem of ZF that each wellordered set corresponds to exactly one ordinal, to which it is isomorphic (see Fact 1.11). If N satisfies ZF and contains $<_R$, then inside N there must be an ordinal $\alpha' \in N$ such that $(\omega, <_R)$ is isomorphic to $(\alpha', \in)$. But this isomorphism would be in V as well (since $N \subseteq V$), and consequently there would be two distinct ordinals in V, α and α', corresponding to $(\omega, <_R)$, and this is a contradiction. $\square$

It follows that in extending the model M we have to avoid adding any binary relation $<_R$ which happens to code an ordinal α between o_M and ω_1 – since they are $\aleph_1$ many of these, this is quite a lot of sets that we must avoid.

3.3.2 The structure of names

Our horizon being limited by the structure M, where we "live", we cannot point to a set which is outside M, but we may give it a *name* inside our model M. Introducing names for the postulated objects outside our universe M has the benefit that we may exercise some level of control over the desired model N; assuming of course that we define the names in such a clever way that we achieve sufficient degree of correspondence between the names and the elements in the desired N.

Obviously, for this approach to work, we must have a sufficient number of names inside our model M; in a way – because our N should be bigger than M – we need more names inside M than is the totality of all the elements of M. But having infinity as our ally, this is easy. Though it is not our official definition of a name, consider the following example.

Example 3.15 For $x \in M$, we will view the pair $\langle x, 0\rangle$ as the canonical name for x.[42] We will also define other names: for $x \in M$, and $n \in \omega$, a

[42] Note that since M satisfies ZF, it is in particular closed under $\langle , \rangle$; hence for $x, y \in M$, also $\langle x, y\rangle \in M$.

pair $\langle x, n\rangle$ will also be a name. Thus, pairs of the type $\langle x, 0\rangle$ will represent the elements of M, while the names $\langle x, n\rangle$ will denote *some other objects* – ideally, the elements in the desired extension $N \supseteq M$. However, notice that the set of all names is a proper subset of M. Indeed, while each $\langle x, n\rangle$ is a member of M, there are certainly sets $y \in M$ which are not ordered pairs, and consequently are not names.

Our official definition of names will be more technical, but the basic idea of the previous example will be preserved, i.e. we will have some special names denoting the elements of M, and in addition we will have other names which will denote the elements of the extension N.

Before plunging into definitions, we mention one more ingredient which will be used in defining the names. Since forcing is a very general technique, it cannot do to have a single class of names that would work equally well for all possible extensions; it is reasonable to expect that the model where $\neg$CH holds may be quite different to the model where $\neg$AC holds. Accordingly, our names will be defined with respect to a given set of *parameters* $\mathbb{P}$, with $\mathbb{P} \in M$. From the technical point of view, $\mathbb{P}$ will be a partially ordered set with a greatest element $1_{\mathbb{P}}$, while the elements $p \in \mathbb{P}$ will be called *conditions.*

Remark. Though the following exposition works equally well with arbitrary partially ordered sets $\mathbb{P}$, we will fix one concrete example $\mathrm{Add}(\omega, 1)$ of such a set of condition $\mathbb{P}$ to make the exposition more transparent.

Definition 3.16 *The domain of the partially ordered set* $\mathrm{Add}(\omega, 1)$ *will contain all finite sequences of* 0 *and* 1*; for instance* $p = \langle 1, 0, 1, 1\rangle$ *is an example of such a sequence. The conditions in* $\mathrm{Add}(\omega, 1)$ *will be ordered by end-extension; if p end-extends q,*[43] *we write* $p \leq q$.[44] *Note that the greatest element of* $\mathrm{Add}(\omega, 1)$ *is the emptyset* $\emptyset$.

To anticipate a little, the name "Add" suggests that the corresponding extension N will "add" (at least) one new subset of ω.

We will now define the class of names $M^{\mathrm{Add}(\omega,1)} \subseteq M$ with respect to the partially ordered set $\mathrm{Add}(\omega, 1)$. The reader will find it helpful to think about the conditions $p \in \mathrm{Add}(\omega, 1)$ as parameters which say to what extent the given name has the right to be in the desired extension N.

[43] For instance $\langle 1, 0, 1, 1\rangle$ end-extends $\langle 1, 0, 1\rangle$.

[44] The reader should notice that p is "less than" q if it is "stronger" in the sense that it contains more information. This usage may seem confusing at first; it can be defended by the argument that the "stronger" a condition is, the more things it prohibits, and consequently restricts the number of suitable models. Compare this with Theorem 3.22.

Definition 3.17 *Adapting the definition in Foundation axiom, see Definition 2.2, we will define (inside M) the class of names $M^{\mathrm{Add}(\omega,1)}$ as follows:*

$$\begin{aligned}
M_0^{\mathrm{Add}(\omega,1)} &= \emptyset \\
M_{\alpha+1}^{\mathrm{Add}(\omega,1)} &= \mathscr{P}(M_\alpha^{\mathrm{Add}(\omega,1)} \times \mathrm{Add}(\omega,1)) \\
M_\lambda^{\mathrm{Add}(\omega,1)} &= \textstyle\bigcup_\alpha M_{\alpha<\lambda}^{\mathrm{Add}(\omega,1)}, \text{ for } \lambda \text{ limit} \\
M^{\mathrm{Add}(\omega,1)} &= \textstyle\bigcup_{\alpha\in\mathrm{On}} M_\alpha^{\mathrm{Add}(\omega,1)}.
\end{aligned}$$

General names will be denoted by letters with a dot above it, as in $\dot{x} \in M^{\mathrm{Add}(\omega,1)}$.

Also, we will single out canonical *names for elements in M. For $x \in M$, the canonical name $\check{x}$ is defined by recursion as follows:*

$$\check{x} \;=\; \{\langle \check{y}, \emptyset\rangle \,|\, y \in x\},$$

where $\check{y}$ is defined in the earlier stage of construction.

Recall that $\emptyset$ is the greatest element of $\mathrm{Add}(\omega,1)$ in the ordering $\leq$ for $\mathrm{Add}(\omega,1)$. Thus, if $\mathbb{P}$ is an arbitrary partially ordered set with a greatest element $1_{\mathbb{P}}$, this element would be in place of $\emptyset$ in the definition of a canonical name.

Example 3.18 The following are examples of names. $\emptyset$ is a name as it is in $M_1^{\mathrm{Add}(\omega,1)}$. Notice that names are some relations R, where if $\langle x, y\rangle \in R$, x is a name defined in the previous stages of the construction, and y is an element of $\mathrm{Add}(\omega,1)$. Accordingly, $\{\langle \emptyset, \langle 0,1\rangle\rangle\}$, $\{\langle \emptyset, \langle 0,1,1,1,0\rangle\rangle, \langle \emptyset, \langle 0,1\rangle\rangle\}$, and $\{\langle\{\langle \emptyset, \langle 0,1,1,1,0\rangle\rangle\}, \langle 0,1,1\rangle\rangle\}$ are all names.

As for the canonical names, a canonical name for $\emptyset$ is just $\emptyset$, for $1 = \{\emptyset\}$, the canonical name is $\{\langle \emptyset, \emptyset\rangle\}$, and so on.

Notice that the basic idea of the definition of both the general and the canonical names does correspond to the simple example in 3.15; the important difference is that instead of the parameters in ω, as in 3.15, we use more complicated parameters in $\mathrm{Add}(\omega,1)$; also to ensure transitivity of the desired model N, we require that members of the names are themselves names – in example 3.15 we ignored the issue whether the x in $\langle x, n\rangle$ is itself a name or not.

3.3.3 Making names into objects

We have shown in Lemma 3.14 that we must be very careful about the elements we will add to our extended universe N. We also mentioned that the crux of the forcing technique is to build the desired extension N around a carefully chosen element x – an element which is new, i.e. lies outside M, but simultaneously avoids to contain "unwanted" information, such as the relation $<_R$ in Lemma 3.14.

In the standing terminology, this new element is called a *generic object*, to be denoted G, and the extension N will be denoted as $M[G]$, i.e. the least model $N \supseteq M$, such that $G \in N$. G will always be some subset of the set of conditions $\mathbb{P}$. Considering the set of conditions $\mathrm{Add}(\omega, 1)$ in our example, the generic object G will determine a new subset of ω – i.e. G will be composed of sequences $p \in \mathrm{Add}(\omega, 1)$ such that for all $p, q \in \mathrm{Add}(\omega, 1)$, either $p \leq q$ or $q \leq p$; in particular, if the conditions in G are put one after the other, they will form a characteristic function of a subset of ω. If $p \in G$, we think about p as a *finite approximation* of the generic object. It must be emphasized that while $G \subseteq \mathrm{Add}(\omega, 1) \subseteq M$, G itself is required to be outside the model M.[45] Figuratively, while M contains all letters (i.e. finite approximations $p \in \mathrm{Add}(\omega, 1)$) necessary to determine the ideal object, the infinite *word* which is composed of these letters (the object G) lies outside the scope of people living in M.

We will describe how to select a generic object G later in the text. For now, assume we have chosen some $G \subseteq \mathrm{Add}(\omega, 1)$ which determines a new subset G of ω; for technical reasons, assume furthermore that $\emptyset \in G$. We will show how the universe $M[G]$ can be described.

Definition 3.19 *An interpretation $\dot{x}_G$ of a name $\dot{x} \in M^{\mathrm{Add}(\omega,1)}$ is defined by recursion as follows.*

$$\dot{x}_G \quad = \quad \{\dot{y}_G \,|\, \exists p \in G \, \langle \dot{y}, p\rangle \in \dot{x}\},$$

where $\dot{y}_G$ is defined in the earlier stages of the construction.

We set

$$M[G] = \{\dot{x}_G \,|\, \dot{x} \in M^{\mathrm{Add}(\omega,1)}\}.$$

Remark. Notice that the definition of $\dot{x}_G$ makes specific the hint given before Definition 3.17, namely that the conditions $p \in \mathrm{Add}(\omega, 1)$ determine how much "right" has the specific $\dot{x}$ to be in $M[G]$ – if it has some $p \in G$ next to itself, it can get into the universe $M[G]$, if it has no such $p \in G$, it may not. This rather vague comment is illustrated by some examples:

Example 3.20 Assume that our G contains (among other sequences) the sequences $\emptyset$, $\langle 0, 1\rangle$, and doesn't contain $\langle 0, 0\rangle$.

We will show some examples how the names are interpreted. Let $x \in M$ be an arbitrary element in M, $\dot{y}_0 = \{\langle\emptyset, \langle 0, 1\rangle\rangle\}$, $\dot{y}_1 = \{\langle\emptyset, \langle 0, 1\rangle\rangle, \langle\emptyset, \langle 0, 0\rangle\rangle\}$,

[45] Since M is countable, it contains at most countably many subsets of ω available in V; due to Cantor theorem 1.2, there are $2^\omega > \omega$ subsets of ω in V. It follows that we have a lot of candidates to choose from when determining the generic object $G \subseteq \mathrm{Add}(\omega, 1)$.

$\dot{y}_2 = \{\langle \emptyset, \langle 0, 0\rangle\rangle\}$, and finally $\dot{g} = \{\langle \check{p}, p\rangle \,|\, p \in \mathrm{Add}(\omega, 1)\}$. Then the interpretation is as follows:

$$\begin{array}{rcl} \check{x}_G & = & x \\ (\dot{y}_0)_G & = & \{\emptyset\} \\ (\dot{y}_1)_G & = & \{\emptyset\} \\ (\dot{y}_2)_G & = & \emptyset \\ \dot{g}_G & = & G. \end{array}$$

Some comments are in order here. The fact that the canonical names $\check{x}$ are always realized by x follows (by induction) from the requirement that $\emptyset \in G$. The interpretation of $\dot{y}$'s is determined by the presence, or absence of $\langle 0, 1\rangle \in G$. As for $\dot{g}_G$, we reason as follows:

$$\dot{g}_G = \{\check{p}_G \,|\, \exists p \in G \, \langle \check{p}, p\rangle \in G\} = \{p \,|\, p \in G\} = G.$$

The rationale behind the definition of the names $M^{\mathrm{Add}(\omega,1)}$ was to ensure we can "talk" about the elements of $M[G]$ inside our model M; in this connection it is instructive to realize that a *single* name $\dot{g}$ always denotes the generic object G, irrespective of what the object G in fact is.[46]

In the following sections we shall show that this uniformity between the model M and the extension $M[G]$ can be taken much further.

3.3.4 Choosing the generic object

The selection of the generic object $G \subseteq \mathrm{Add}(\omega, 1)$ is determined by the requirement that the model $M[G]$ should satisfy all the axioms of ZF. Taking into account that each $p \in G$ is in M and should function as a finite approximation of G, the ideal situation would be the following:

Let $\varphi(v_0, \ldots)$ be an arbitrary formula and let it be true in $M[G]$ under the interpretations $(\dot{x}_0)_G, \ldots$, i.e.

$$M[G] \models \varphi[(\dot{x}_0)_G, \ldots].$$

Then there is some $p \in G$, a finite approximation of G, such that

$$p \text{ "decides" } \varphi(\dot{x}_0, \ldots) \text{ inside } M.$$

The nature of the "deciding" needs more clarification, but the intuitive idea is clear: not only we can refer to particular objects, such as different G's,

[46] Without giving details, there exist (in V) 2^ω many generic objects in total for any "interesting" $\mathbb{P}$ – and $\mathrm{Add}(\omega, 1)$ is interesting in this sense, i.e. there is a sequence $\langle G_\alpha \,|\, \alpha \in 2^\omega\rangle$ of generic objects existing in V; $\dot{g}$ denotes in each extension $M[G_\alpha]$ exactly the object G_α, i.e. $\dot{g}_{G_\alpha} = G_\alpha$ for every α.

with a single name, i.e. $\dot{g}$, we can also decide each property holding in $M[G]$ by an element which exists in M, i.e. some $p \in G \subseteq \mathrm{Add}(\omega, 1)$. Notice that this is a priori not contradictory: although we can decide each property with an element in M, there are infinitely many properties to decide – but this would require to know which infinitely many objects $p \in \mathrm{Add}(\omega, 1)$ *do the deciding*; in other words it would require that we know (inside M) the whole $G \subseteq \mathrm{Add}(\omega, 1)$. This leads up to the following central definition and a theorem.

Definition 3.21 *We say that* $p \in \mathrm{Add}(\omega, 1)$ forces[47] $\varphi(\dot{x}_0, \ldots)$*, in symbols*

$$p \Vdash \varphi(\dot{x}_0, \ldots),$$

if for every generic object $G \subseteq \mathrm{Add}(\omega, 1)$*, if* $p \in G$*, then*

$$M[G] \models \varphi[(\dot{x}_0)_G, \ldots].$$

Theorem 3.22 (Correspondence theorem) *If G denotes a generic object for* $\mathrm{Add}(\omega, 1) \in M$ *and $\dot{x}_0 \ldots$ are arbitrary names, then the following is true:*

$$M[G] \models \varphi[(\dot{x}_0)_G, \ldots] \text{ iff } \exists p \in G\, p \Vdash \varphi(\dot{x}_0, \ldots).$$

A proof of this theorem is well outside the scope of this article. But some intuitive arguments will be given in the rest of this section.

The name "forcing" in Definition 3.21 signifies that p forces some formula, or property, to hold in the generic extension $M[G]$, *irrespective* of what the object G in fact is. However, notice that Definition 3.21 is really just a definition: the main import of the forcing relation $\Vdash$, in correspondence with the motivation given at the beginning of this section, should be that it is expressible inside M; this is similar to the name $\dot{g}$ for the generic object – recall that the name $\dot{g}$ exists inside M. Accordingly, the hardest task in verifying the properties of forcing is to show that the relation $\Vdash$ in Definition 3.21 is in fact definable inside M. In Definition 3.25, we show how the relation $\Vdash$ is defined for the existential quantifier.

As suggested earlier, the members $p \in \mathrm{Add}(\omega, 1)$ can be viewed as finite approximations of the extension $M[G]$; Theorem 3.22 in fact claims that these finite approximations decide everything about the extension $M[G]$. Given $p \in G$, there are some properties φ which p decides, but there are some other which are left undecided by p. If $q \leq p$, i.e. if q is stronger than p, then

[47]This relation has given its name to the entire technique, called "forcing".

q should intuitively decide all properties which p does, and possibly some additional properties as well.[48]

Example 3.23 If q is stronger than p, then q should "know" more than p does, and moreover if $p \Vdash \exists x\, \varphi$, then it is reasonable to expect that there is some witness $\dot{x}$ for φ, such that $q \Vdash \varphi(\dot{x})$.[49] It turns out that it would be too strong to demand that such a witness exists for every $q \leq p$; however, *eventually*, each $q \leq p$ should have such a witness. This leads to the following definition.

Definition 3.24 *Let $D \in M$; we say that $D \subseteq \mathrm{Add}(\omega, 1)$ is* dense *if*

$$\forall p \in \mathrm{Add}(\omega, 1)\, \exists d \in D \text{ such that } d \leq p.$$

For $p \in \mathrm{Add}(\omega, 1)$, we say that D is dense below p *iff*

$$\forall p' \leq p\, \exists d \in D \text{ such that } d \leq p'.$$

Definition 3.25 *The inductive definition of $\Vdash$ for an existential quantifier is as follows:*

$$p \Vdash \exists x\, \varphi \text{ iff the set } \{q \leq p \mid \exists \dot{x}\, q \Vdash \varphi(\dot{x})\} \text{ is dense below } p.$$

It turns out that the concept of "being dense below a condition" is the correct apparatus which is used in defining the forcing relation $\Vdash$ for an arbitrary formula φ. If σ is a sentence in the forcing language, we actually obtain the following nice property: the set of all p such that p decides σ, i.e. $p \Vdash \sigma$ or $p \Vdash \neg\sigma$ is dense in $\mathrm{Add}(\omega, 1)$.

We will now turn to the definition of a generic object G where the concept of denseness is also crucial.

Definition 3.26 *A subset $G \subseteq \mathrm{Add}(\omega, 1)$ is a generic object if it satisfies the following conditions:*

(i) The greatest element of $\mathrm{Add}(\omega, 1)$, i.e. $\emptyset$, is in G;
(ii) If $p \in G$ and $p \leq q$, then $q \in G$;

[48] To a reader familiar with models for intuitionistic logic, this property of the forcing relation may seem very similar to a Kripke frame; there are some important analogies, but some important distinctions as well. For such a reader, to construe members of $\mathbb{P}$ as possible worlds may help to grasp intuitively what is going on. The book [Fit69] studies in detail this analogy.

[49] Recall that $\Vdash$ is about semantics, not syntax; this should be understood as follows, if an arbitrary theory T proves the formula $\exists x\, \varphi$, then it doesn't have to be the case that there is a term t_x such that $T \vdash \varphi(t_x)$; on the other hand, if M is a model of T, then $M \models \exists x\, \varphi$ does imply that there is a member $m_x \in M$ such that $M \models \varphi(m_x)$. The definition of $\Vdash$ should therefore take this into account.

(iii) If $p, q \in G$, then there is some $r \in G$ such that $r \leq p$, and $r \leq q$;

(iv) If $D \in M$ is a dense subset of $\mathrm{Add}(\omega, 1)$, then there is some $d \in G$ such that $d \in D$.

Some comments are in order here. Technically speaking, the first three conditions imply that G is a filter – it is easy to show that there are many G's satisfying these three conditions which exist in M. It is the fourth condition of denseness which makes sure that G cannot exist in M; see Lemma 3.29.

Theorem 3.27 (Existence of a generic object) *If M is countable transitive set with $\mathrm{Add}(\omega, 1) \in M$, then there is a set $G \in V$ such that G is a generic object for $\mathrm{Add}(\omega, 1)$. In general, the same applies to an arbitrary partial order $\mathbb{P} \in M$.*

Proof. Since M is countable, there are only countably many dense sets $D \subseteq \mathbb{P}$ existing in M. Let $\langle D_n \,|\, n < \omega \rangle$ be their enumeration. Let $p_0 \in \mathbb{P}$ be an arbitrary element. By induction construct a decreasing sequence $p_{n+1} \leq p_n$ such that $p_{n+1} \in D_n$. Set

$$G = \{p \in \mathbb{P} \,|\, \exists p_n \, p_n \leq p\}.$$

It is not hard to verify that G satisfies all the required properties.

Notice the importance of the countability of M in the proof. If M were not countable, then the construction could fail at a limit step: for the decreasing sequence of p_n for $n \in \omega$, there might exist no p_ω below all of them. $\square$

Example 3.28 We say that $\mathbb{P}$ is *non-trivial* if for all $p \in \mathbb{P}$ there are $q_0, q_1 \in \mathbb{P}$ such that $q_0 \leq p$ and $q_1 \leq p$ and q_0, q_1 don't have a common stronger condition; i.e. there is no r such that $r \leq q_0$ and $r \leq q_1$. This is denoted as $q_0 \perp q_1$ and we say that q_0, q_1 are incompatible; this name clearly refers to the fact that there can be no generic object G which will contain both q_0 and q_1. Notice that $\mathrm{Add}(\omega, 1)$ is non-trivial in this sense.

Lemma 3.29 *If $\mathbb{P}$ is non-trivial, then no generic object is a member of M.*

Proof. By contradiction. If $G \in M$, then in view of Definition 3.26, item (iv), it is enough to show that the set $D_G = \{p \in \mathbb{P} \,|\, p \notin G\}$ is dense in $\mathbb{P}$ (since G is in M by our assumption, D_G is in M as well; if D_G were dense, then there is some $p \in G$ in D_G, contradicting the definition of D_G). But this is easy: assume $p \in \mathbb{P}$ is arbitrary and q_0, q_1 are two incompatible conditions below p; since q_0, q_1 cannot be both in G, one of them is in D_G. $\square$

We will now illustrate the importance of the condition (iv) in Definition 3.26 which demands that G meets all dense subsets of $\mathrm{Add}(\omega, 1)$ (or $\mathbb{P}$ in general).

Corollary 3.30 *If G is a generic filter for* $\mathrm{Add}(\omega, 1)$*, then $M[G]$ contains a new subset of ω.*

Proof. Work in M and define for each $n \in \omega$ a set $D_n = \{p \in \mathrm{Add}(\omega, 1) \mid n \in \mathrm{dom}(p)\}$. Obviously, each D_n is dense: if $q \in \mathrm{Add}(\omega, 1)$ is arbitrary, we can always find some $p \leq q$ such that n is in the domain of p.

Let G be a generic filter for $\mathrm{Add}(\omega, 1)$. Define $g(n) = 1$ if there is some $p \in G$ such that $p(n) = 1$; define $g(n) = 0$ otherwise. As D_n is dense for each $n \in \omega$, g is defined on all elements of ω. Note that if $p(n) = 1$ for some $p \in G$, then there can be no other $q \in G$ such that $q(n) = 0$, by the condition (iii) in Definition 3.26, and so g is correctly defined.

We claim that g is a new subset of ω. By Lemma 3.29, G cannot be in M; if g were in M, so would be G as G is definable from g: $G = \{p \in \mathrm{Add}(\omega, 1) \mid p \text{ is compatible with } g\}$.[50] It follows that $g \in M[G] \setminus M$. $\square$

We shall end this section with a general theorem which says that for *every* forcing $\mathbb{P}$ and *every* generic filter $G \subseteq \mathbb{P}$, the resulting model $M[G]$ satisfies ZF(C).

Theorem 3.31 *For any partially ordered set $\mathbb{P} \in M$ and any generic object $G \subseteq \mathbb{P}$, $M[G]$ satisfies all axioms of ZF; if M satisfies also the axiom of choice, AC, so does $M[G]$. In particular, if φ is an axiom of ZF(C), then $1_{\mathbb{P}} \Vdash \varphi$, where $1_{\mathbb{P}}$ is the greatest element in $\mathbb{P}$.*

The proof of the theorem requires a rigorous treatment of the forcing relation. It must suffice to say that the main tool used in the proof is the fact that the forcing relation $\Vdash$ is definable in M and consequently to make sure φ holds in $M[G]$ we can use that some formulas relevant to φ hold in M, as M is a model of ZF(C).

To prevent misunderstanding, however, it must be emphasized that while the truth of AC in M does imply that AC holds in $M[G]$, this is by no means true for an arbitrary formula φ. In particular, by nature of the forcing construction, $M[G]$ can never satisfy $V = L$ if G is not in M,[51] while M can satisfy $V = L$, and in practice it often does.

The combination of Theorem 3.31 and Corollary 3.30 gives the following theorem:

Theorem 3.32 *If ZF is consistent, so is ZF + $V \neq L$.*

[50] This does require some more detailed argument which we omit.

[51] Since the ordinal height of M and $M[G]$ is the same, it holds that $L^M = L^{M[G]}$. It follows that $L^M \subseteq M \subsetneq M[G]$, and this contradicts $V = L$ in $M[G]$. See also Theorem 3.32.

Proof. Let M be a ground model satisfying ZF. Let $M[G]$ be a generic extension for $G \subseteq \mathrm{Add}(\omega, 1)$. By Theorem 3.31, $M[G]$ satisfies ZF. By Corollary 3.30, $M[G]$ cannot satisfy $V = L$ as the the new set $g \subseteq \omega$ derived from G (see Corollary 3.30) is certainly not in L (recall that $L = L^M = L^{M[G]} \subseteq M \subsetneq M[G]$). $\square$

Notice that Theorem 3.32 is already non-trivial. By Theorem 3.12, we cannot construct an inner model to show consistency of $V \neq L$ (just replace $\neg CH$ in the proof of Theorem 3.12 by $V \neq L$).

3.3.5 Making CH false

By Corollary 3.30, forcing with $\mathrm{Add}(\omega, 1)$ adds a new subset g of ω. In fact, since $M[G]$ satisfies ZF, many more subsets of ω will be added into $M[G]$; for instance for any $n \in \omega$, g above n is a new subset. But to make sure CH fails in $M[G]$, we need to add at least $\aleph_2$ many new subsets. It can be shown, however, that $\mathrm{Add}(\omega, 1)$ will not add as many new sets.

An obvious strategy to add at least $\aleph_2$ many new subsets of ω is to apply $\mathrm{Add}(\omega, 1)$ $\aleph_2$-many times.

Theorem 3.33 *There exists a partial order* $\mathrm{Add}(\omega, \aleph_2)$*, namely, roughly speaking,* $\aleph_2$*-many copies of* $\mathrm{Add}(\omega, 1)$ *put one after the other, such that if G is generic for* $\mathrm{Add}(\omega, \aleph_2) \in M$*, then* $M[G]$ *satisfies* $2^{\aleph_0} = \aleph_2$*, i.e.* $\neg CH$*. In particular, in view of Theorem 3.10, CH is independent on the axioms of ZF, and ZFC.*

We will not give a rigorous proof, but will address instead some finer technical points which are important for the practical applications of the forcing technique, and in particular for the failure of CH. Notice that the development of forcing described above works for an *arbitrary* partial order $\mathbb{P}$ (we have used the example of $\mathrm{Add}(\omega, 1)$ but in fact we used none of its specific properties so far). It is clear, however, that some properties of the forcing extension must depend on the specific properties of the given partial order. In Section 3.1, we mentioned that the concept of a cardinal number is *not* absolute for transitive models of ZF. In other words, it may happen that some cardinal numbers in M are destroyed, or are *collapsed* in the standing terminology, in $M[G]$ after forcing with some partial order $\mathbb{P}$ (if $\kappa < \lambda$ are cardinals in M, a forcing $\mathbb{P}$ may add a 1-1 function from κ onto λ, collapsing λ). Although we may sometimes wish to collapse cardinals, it is not difficult to see that in the case of Theorem 3.33 and the partial order $\mathrm{Add}(\omega, \aleph_2)$ we had better avoid collapsing. The reason is that $\mathrm{Add}(\omega, \aleph_2)$ adds $\aleph_2$-many new subsets of ω, where $\aleph_2$ (i.e. the second uncountable cardinal) is calculated in M. If for instance $\aleph_1$ is collapsed in $M[G]$ (and $\aleph_2$ is not collapsed), then

$\aleph_2$ of M becomes in fact the *first* uncountable cardinal in $M[G]$, i.e. $\aleph_1$ of $M[G]$, and this would mean that CH again holds in $M[G]$!

Here we come to the crucial task which concerns practical application of forcing: one needs to carefully verify various properties of the partial order $\mathbb{P}$ to make sure that $\mathbb{P}$ achieves the right thing. By way of illustration, we show how to ensure that the cardinal $\aleph_1$ of M is not collapsed.

Lemma 3.34 $\mathrm{Add}(\omega, 1)$ *doesn't collapse* $\aleph_1$ *of* M*.*

Sketch of proof. It is enough to show that if G is a generic filter for $\mathrm{Add}(\omega, 1)$, then in $M[G]$ there is no countable subset X cofinal in the ordinal $\aleph_1$. In detail, if we denote $\gamma = \aleph_1$ then in $M[G]$ there can be no increasing sequence of ordinals $X = \langle x_n \,|\, n \in \omega\rangle$ such that the limit of $\langle x_n \,|\, n \in \omega\rangle$ is γ (if there were such a sequence in $M[G]$, then it easily follows that γ cannot be the first uncountable cardinal in $M[G]$).

We will proceed by contradiction. Assume that there is in $M[G]$ some such sequence $X = \langle x_n \,|\, n \in \omega\rangle$ cofinal in $\gamma = \aleph_1$ of M. By Correspondence theorem 3.22, there is some $p \in \mathrm{Add}(\omega, 1)$ such that $p \Vdash (\dot{X}$ is a cofinal sequence in $\check{\gamma})$, where $\dot{X}$ is a name for the sequence $X = \langle x_n \,|\, n \in \omega\rangle$. The first element of the sequence X, i.e. x_0, has some name $\dot{x}_0$ pertaining to it. As it is a name, it may be interpreted by different ordinal numbers under different generic filters G; but whichever ordinal it is (in a given generic extension), it has to be forced by some condition to be this ordinal, again by Correspondence theorem 3.22. However, $\mathrm{Add}(\omega, 1)$ has only size ω, and consequently $\dot{x}_0$ can represent only countably many ordinals below $\aleph_1$. The same applies to $\dot{x}_n$ for every $n \in \omega$. This means that we can find *inside* M some countable family of ordinals below $\aleph_1$ which contains all the possible ordinals which can be represented by the names $\dot{x}_n$. But as $\aleph_1$ is really uncountable in M, no such family existing in M can be cofinal in it. This is a contradiction. $\square$

Notice that the argument in the previous lemma used the size of the forcing notion to find in M some countable family of ordinals which may by interpreted by the names $\dot{x}_n$. The forcing notion $\mathrm{Add}(\omega, \aleph_2)$ in Theorem 3.33 (which we have defined very vaguely) is certainly bigger than ω. We will show that this obstacle can be overcome by a more detailed analysis of the forcing relation.

Definition 3.35 *Let* $\mathbb{P}$ *be a partial order. A subset* A *of* $\mathbb{P}$ *is called an* antichain *if all elements of* A *are pairwise incompatible, i.e. for all* $p, q \in A$, *there is no* $r \in P$ *such that* $r \leq p, r \leq q$*.*

Recall that if $G \subseteq \mathbb{P}$ is a generic filter, than all elements of G must be pairwise compatible. It follows that G can contain at most one element of A.

The partial order $\mathrm{Add}(\omega, \aleph_2)$ can be formally defined in such a way as to satisfy the condition that all antichains in $\mathrm{Add}(\omega, \aleph_2)$ are at most countable. Naively, one would put in $\mathrm{Add}(\omega, \aleph_2)$ all functions p with domain $\omega \times \aleph_2$ and range included in $\{0, 1\}$ such that p restricted to $\alpha < \aleph_2$ is some finite sequence of zeros and ones – just like a condition in $\mathrm{Add}(\omega, 1)$. The idea being that p approximates $\aleph_2$-many new subsets of ω. However, $\mathrm{Add}(\omega, \aleph_2)$ defined in this way contains antichains of uncountable size. It turns out that the right solution is to require that p be non-trivial only at finitely many $\alpha < \aleph_2$, i.e. except for finitely many α, p restricted to a coordinate $\alpha' < \aleph_2$ must in fact be an empty set (empty set is regarded as a trivial finite sequence, and hence the name "non-trivial"). Such p are said to have a *finite support.*

Definition 3.36 *The forcing* $\mathrm{Add}(\omega, \aleph_2)$ *contains all conditions* p *with domain* $\omega \times \aleph_2$ *and range included in* $\{0, 1\}$ *such that the projection of* p *to a coordinate* $\alpha < \aleph_2$ *is a finite sequence of 0's and 1's and* p *has finite support. The relation* $p \leq q$ *is the reverse inclusion:* $p \leq q$ *iff* $p \supseteq q$.

The following fact will be given without a proof.

Fact 3.37 *All antichains in* $\mathrm{Add}(\omega, \aleph_2)$ *are at most countable.*

This Fact allows us to show:

Lemma 3.38 $\mathrm{Add}(\omega, \aleph_2)$ *doesn't collapse* $\aleph_1$ *of* M.

Sketch of proof. The fact that all antichains in $\mathrm{Add}(\omega, \aleph_2)$ are at most countable is enough to infer that $\aleph_1$ is not collapsed in a generic extension $M[G]$ by $\mathrm{Add}(\omega, \aleph_2)$, and consequently CH is false in $M[G]$. Realize that the argument in Lemma 3.34 applies here: if p and q force distinct ordinals for the interpretation of $\dot{x}_n$, then p and q must be incompatible; it follows that they form an antichain, and consequently the number of such p and q can be at most countable – even if $\mathrm{Add}(\omega, \aleph_2)$ itself is bigger. Thus, there is again in M a countable family of ordinals which contains all the possible interpretations of the names $\dot{x}_n$.[52] □

3.3.6 Making AC false

The model for the negation of AC is technically more demanding, so we won't be able to give an intuitive outline of the proof. It must suffice to say that it is possible to construct a forcing extension $M[G]$ and an inner model $N \subseteq M[G]$, where the axiom of choice fails.

[52]Technically speaking, we need to work below a condition p_X that forces that $\dot{X}$ is a sequence of ordinals. If we set $A = \{p \leq p_X \mid \exists \alpha_p \, p \Vdash \dot{X}(n) = \check{\alpha}_p\}$, then the set of distinct α_p's is at most countable as the relevant p's form an antichain.

3.3.7 Forcing: Frequently asked questions

Models or syntax? We have mentioned above that the assumption about the existence of a transitive countable model of ZF is not necessary for the development of forcing. The key properties of forcing which enable us to completely avoid the use of models are the following:

(i) The definability of the relation $\Vdash$ inside M without any recourse to G – and consequently in V as well if we do the definition in V in place of M;

(ii) Preservation of the forcing relation under the provability, see Fact 3.39 below;

(iii) The fact that the definition of the forcing relation rules out the possibility that there exists $p \in \mathbb{P}$ forcing both φ and $\neg\varphi$, where φ is an arbitrary formula.

Fact 3.39 *Assume that $\varphi_0 \wedge \ldots \wedge \varphi_n \vdash \psi$; then if $p \Vdash \varphi_0 \wedge \ldots \wedge \varphi_n$, then it is also true that $p \Vdash \psi$.*

The following lemma shows how to avoid the use of models.

Lemma 3.40 *Let $\mathbb{P}$ be an arbitrary forcing notion. Assume that there is $p \in \mathbb{P}$ such that $p \Vdash \varphi$, then $ZF \nvdash \neg\varphi$.*

Proof. First we have to emphasize that the property $p \Vdash \varphi$ is completely expressible in V, without any recourse to $M[G]$. Recalling that the purpose of forcing is to derive consistency results, the above lemma is entirely sufficient for our needs.

Assume for contradiction that $ZF \vdash \neg\varphi$; then there exist a finite list of axioms of ZF $\varphi_0, \ldots, \varphi_n$ such that

$$\varphi_0 \wedge \ldots \wedge \varphi_n \vdash \neg\varphi.$$

By Theorem 3.31, $1_{\mathbb{P}} \Vdash ZF$; by property in Fact 3.39, we also have $1_{\mathbb{P}} \Vdash \neg\varphi$. We have mentioned above that if $p \leq q$, then p forces at least the same formulas as q does; $p \leq 1_{\mathbb{P}}$ hence implies that $p \Vdash \neg\varphi$. This is a contradiction with the item (iii) above. $\square$

For readers with more familiarity with logic, we can add that the true benefit of the syntactical approach is that we can formulate the consistency results on the level of arithmetics, instead of relying on set theory and its consistency.

Partial orders or Boolean algebras? In many books, in [Bal00] for one, the development of forcing seems intrinsically dependent on (complete) Boolean algebras. This may be a deterring feature for students inadequately familiar with the theory of Boolean algebras; fortunately, the use of Boolean algebras can be completely avoided. Indeed, the incorporation of Boolean algebras into the theory of forcing came only later by work of Vopěnka and Solovay; Boolean algebras add more understanding into the way forcing works, and also provide nice connection to logic. In what follows, we describe very briefly – and in a zig-zag way, in what respect the Boolean algebras are perhaps more natural to use than general partial orders, and also give some argument to show that both approaches are for the most purposes identical. Due to lack of space, however, some familiarity with Boolean algebras must be assumed.

Some simplifications brought in by Boolean algebras appear already in the definition of names. Recall that in the definition of the names in $M^{\mathrm{Add}(\omega,1)}$, see Definition 3.17, if $\dot{x}$ is a name then there can be many elements $p \in \mathrm{Add}(\omega, 1)$ such that $\langle \dot{x}, p\rangle$ is an element of some other name $\dot{y}$. Let us fix a complete Boolean algebra $\mathbb{B}$ with its canonical ordering $<_{\mathbb{B}}$ (and for technical reasons, remove the least element in the ordering $<_{\mathbb{B}}$); then $(\mathbb{B}, <_{\mathbb{B}})$ is a partially ordered set and all the development of forcing can be applied to it (recall that it works for *any* partially ordered set). Assume that there is a name $\dot{y} = \{\langle \dot{x}, p\rangle \,|\, p \in I\}$, where $I \subseteq \mathbb{B}$ is some set. By the standard definition of a name in Definition 3.17, this is a regular name and generally it may not be replaceable by some "simpler" name; now, since $\mathbb{B}$ is a complete Boolean algebra, there exist a supremum $\hat{p} = \bigwedge p_{i \in I}$. It turns out that the name $\dot{y}$ can be equivalently replaced by a name $\dot{y}' = \{\langle \dot{x}, \hat{p}\rangle\}$, i.e. in the sense of forcing relation, all the names p_i can be "approximated" by the greatest weaker element of $\mathbb{B}$, namely the supremum $\hat{p}$. Note that such replacement needs to take place in all names, so unless the Boolean algebra is complete, such replacement cannot be carried out.

Similarly, in the definition of the forcing relation we can use the analogy between the connectives in logic and the operations in the Boolean algebra $\mathbb{B}$ – they are even sometimes denoted by the same symbols: $\wedge, \vee, \neg = {}', \exists$ = infimum, and $\forall$ = supremum. The most important consequence of this analogy is that we may inductively calculate a Boolean value, i.e. an element of $\mathbb{B}$, for each formula $\varphi(\dot{x}_0, \ldots)$. In fact this value may be taken as a generalized truth value attributed to a formula – recall that the usual truth value in logic takes either the value 0 or 1, where $\{0, 1\}$ is a (trivial) complete Boolean algebra. These analogies can be taken much further, but they cannot make the forcing technique more efficient than it already is, as the following – rather vaguely formulated – theorem shows.

Theorem 3.41 *For every partially ordered set $\mathbb{P}$, there is a unique complete Boolean algebra $\mathbb{B}_{\mathbb{P}}$, called the* completion *of $\mathbb{P}$, such that the forcing with $\mathbb{P}$ and $\mathbb{B}_{\mathbb{P}}$ achieves the same thing.*

In practice, it is a matter of personal preferences of the individual mathematicians whether they use the partial order approach, or the Boolean algebra one.[53]

4 Conclusion

In the present article, we have argued that it is in the nature of set theory to be "open-ended" in the sense that many interesting properties, such as AC or CH, can be added into our system both in their positive and negative form.

There are many other topics in set theory which shed more light on the issues discussed in this article. We have, for instance, completely ignored the question of the existence of the so called *large cardinals* which, at least in the hopes articulated by Gödel, see for instance [Göd99], might have had some impact on the intuitive validity or falsity of CH. These issues will be hopefully brought to the reader's attention in the projected second part of this article.

[53] In some special cases, the use of Boolean algebras does lead to new insights, but such examples require a more detailed knowledge of forcing.

References

[Bal00] Petr Balcar, Bohuslav a Štěpánek. *Teorie množin.* Academia, 2000.

[Coh63] Paul J. Cohen. The independence of the continuum hypothesis. *Proc. Natl. Acad. Sci. U.S.A.*, 50, 1963.

[Fit69] M.C. Fitting. *Intuitionistic Logic, Model Theory and Forcing.* North-Holland, 1969.

[Göd38] Kurt Gödel. The consistency of the axiom of choice and the generalized continuum hypothesis. *Proc. Natl. Acad. Sci. U.S.A.*, 24, 1938.

[Göd99] Kurt Gödel. *Filosofické eseje.* OIKOYMENH, 1999.

[Jec03] Tomáš Jech. *Set Theory.* Springer, 2003.

[Kun80] Kenneth Kunen. *Set Theory: An Introduction to Independence Proofs.* North Holland, 1980.

[Zer04] E. Zermelo. Beweis, dass jede menge wohlgeordnet werden kann. *Math. Ann.*, 59, 1904.