Set Theory and the Foundation of Mathematics

June 19, 2018

Basics

We have:

- Relations (subsets on their domain)
- Ordered pairs:

Definition

The ordered pair $\langle x, y \rangle$ is the set $\{\{x, y\}, \{x\}\}$.

- Cartesian products $A \times B$
- Functions:

Definition

A function $f : A \to B$ is a relation $f \subseteq A \times B$ such that $\forall x \in A \; \exists! y \in B \; \langle x, y \rangle \in f$. We write $f(a)$ for the unique $b \in B$ such that $\langle a, b \rangle \in f$.

- The set ω of "natural numbers", containing $0 := \varnothing$ and for each $n \in \omega$ the set $S(n) := n \cup \{n\}$.

Inductive Definitions

Theorem (Recursion Theorem for $\mathbb{N}$)

For any $g : A \to B$ and $h : A \times \omega \times B \to B$, there is a unique function $f : A \times \omega \to B$ such that for all $a \in A$ and $n \in \omega$:

$$f(a, 0) = g(a) \qquad \text{and} \qquad f(a, S(n)) = h(a, n, f(a, n))$$

Example

For all $a, b, n \in \omega$ we let $g(a) = a$ and $h(a, n, b) = S(b)$. Then the f postulated by the recursion theorem satisfies $f(a, 0) = a$ and $f(a, S(n)) = h(a, n, f(a, n)) = S(f(a, n))$ – i.e. $f(a, n)$ is exactly the function $a + n$.

Hence, we can inductively define addition, multiplication and exponentiation on ω.

Equivalence Relations

How do we get the other number spaces?

Definition

- An **equivalence relation** on a set A is a relation $R \subseteq A \times A$ such that R is reflexive, symmetric and transitive.
- Given an equivalence relation $R \subseteq A \times A$ and $a \in A$, we call the set $[a]_R := \{x \in A | R(x, a)\}$ the **equivalence class** of a.
- We call a set $X \subseteq A$ such that $\forall a \in A \; \exists! x \in X \; R(x, a)$ a **representative system** of R.

Theorem

In ZF, the axiom of choice is equivalent to the statement that every equivalence relation has a representative system

(In practice the axiom of choice is often not necessary to construct a representative system)

Definition

- Let $\sim \subseteq \omega^2 \times \omega^2$ such that $\langle a_1, a_2 \rangle \sim \langle b_1, b_2 \rangle :\Leftrightarrow a_1 + b_2 = b_1 + a_2$. Note that $\sim$ is an equivalence relation.
- We define $\mathbb{Z}$ as any representative system of $\sim$.

Definition

- Let $Z := \mathbb{Z} \times (\omega \setminus 0)$ and $\sim \subseteq (\mathbb{Z} \times Z)^2$ such that $\langle a_1, a_2 \rangle \sim \langle b_1, b_2 \rangle :\Leftrightarrow a_1 \cdot b_2 = b_1 \cdot a_2$. Note that $\sim$ is an equivalence relation.
- We define $\mathbb{Q}$ as any representative system of $\sim$.

Definition

- Let $\mathbb{Q}^C$ be the set of Cauchy sequences over $\mathbb{Q}$ and $\sim \subseteq (\mathbb{Q}^C) \times (\mathbb{Q}^C)$ such that $(a_n) \sim (b_n) :\Leftrightarrow \lim_{n \mapsto \infty} a_n - b_n = 0$. Note that $\sim$ is an equivalence relation.
- We define $\mathbb{R}$ as any representative system of $\sim$.

Counting Past Infinity

Remember: $0 = \varnothing$, $1 = 0 \cup \{0\} = \{0\}$, $2 = 1 \cup \{1\} = \{0, 1\}, \ldots$
ω =The union of "all those numbers" (smallest set containing $\varnothing$ and closed under $S(x) = x \cup \{x\}$)

...what if we just continue?

$$S(\omega) = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\} = \omega + 1$$

$$S(\omega + 1) = \{0, 1, \ldots, \omega, \omega + 1\} = \omega + 2, \omega + 3, \omega + 4, \ldots$$

$$\omega + \omega = \underbrace{\bigcup_{n \in \omega} (\omega + n)}_{\text{"limit"}} = \omega \cdot 2, \omega \cdot 3, \ldots, \omega \cdot \omega = \omega^2, \omega^3, \ldots$$

$$\ldots, \omega^\omega, \omega^{\omega^\omega}, \ldots, \bigcup_{n \in \omega} \underbrace{\omega^{\cdot^{\cdot^{\cdot^{\omega}}}}}_{n \text{ times}} = \varepsilon_0, \varepsilon_0 + 1, \ldots$$

...we get **Ordinal numbers**! (Note that all of these here are countable)

Ordinal Numbers

Definition

A **well-order** $<$ on S is a total order on S such that every subset of S has a minimal element.
Equivalently: ...such that every element in S is either maximal or has a unique successor.

$\Rightarrow$ We can "count" well-ordered sets using a successor function and "limit steps" (such as ω, which is the "limit" of the natural numbers).

Definition

A set is called **ordinal number** if it is transitive ($\in$-closed) and well-ordered by $\in$. The (proper) class of all ordinal numbers is called **On** (definable).
A set is called **natural number** if it is transitive and well-ordered by both $\in$ and $\in^{-1}$.

Transfinite Induction

Theorem (Recursion Theorem for On)

For every $\mathbf{F} : \mathbf{V} \to \mathbf{V}$, *there exists a unique* $\mathbf{G} : \mathbf{On} \to \mathbf{V}$ *such that* $\forall \alpha \in \mathbf{On}\ \mathbf{G}(\alpha) = \mathbf{F}(\mathbf{G} \restriction \alpha)$.

This allows for an induction/recursion principle on **On**:
Every ordinal α is either

1. $\alpha = \varnothing$ or
2. $\alpha = \beta + 1$ for some $\beta \in \mathbf{On}$ or
3. α is a limit ordinal $\bigcup_{\beta<\alpha} \beta$.

Example

Define addition inductively on **On** by: $\alpha + 0 = \alpha$,
$\alpha + S(\beta) = S(\alpha + \beta)$ and for limit numbers λ: $\alpha + \lambda = \bigcup_{\beta<\lambda}(\alpha + \beta)$

Y tho?

Theorem

Every well-order is isomorphic to an ordinal.

Theorem (Zermelo's Well-Ordering Theorem)

In ZF, the axiom of choice is equivalent to the statement that every set can be well-ordered.

$\Rightarrow$ Ordinal numbers form a "representative class" of all sets (under equivalent well-orders)

Note: We can never construct a well-order of e.g. the real numbers, but by the axiom of choice one has to exist. Without the axiom of choice, $\mathbb{R}$ is not (necessarily) well-orderable.

Aside: The Axiom of Determinacy

Definition (Game)

Let $A \subseteq \omega^\omega$. Players P_A and P_B alternate in picking a natural number n_i, producing a sequence $r = (n_0, n_1, n_2, \ldots)$. Player P_A wins, iff $r \in A$. A strategy is a function $f : \omega^{<\omega} \to \mathbb{N}$. A winning strategy for player P is a strategy that guarantees a win for P.

Definition (Axiom of Determinacy)

AD is the statement that for every $A \subseteq \omega^\omega$, either Player P_A or P_B has a winning strategy for A.
AD is equivalent to

$$(\exists r_0 \forall r_1 \exists r_2 \ldots r \in A) \vee (\forall r_0 \exists r_1 \forall r_2 \exists r_3 \ldots \neg r \in A)$$

Theorem

ZF+AD implies that $\mathbb{R}$ is not well-orderable.

The Von Neumann Hierarchy

Definition (The Von Neumann Hierarchy)

Let

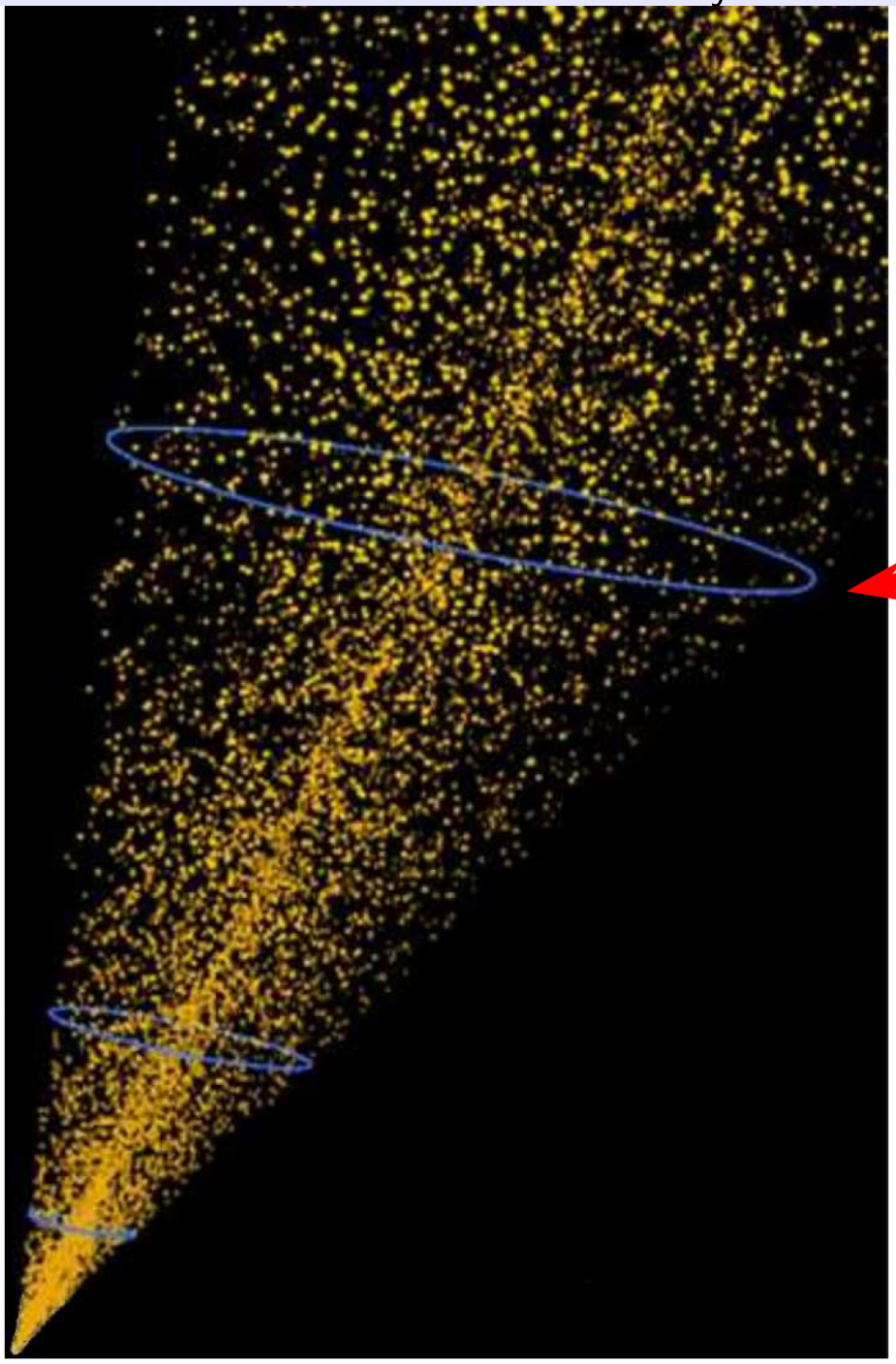
- $\mathbf{V}_0 := \varnothing$
- For any ordinal α we let $\mathbf{V}_{\alpha+1} := \mathcal{P}(\mathbf{V}_\alpha)$
- For any limit ordinal λ we let $\mathbf{V}_\lambda := \bigcup_{\alpha<\lambda} \mathbf{V}_\alpha$

Theorem

In ZF$^-$ (ZF without the axiom of foundation), the axiom of foundation is equivalent to $\mathbf{V} = \bigcup_{\alpha\in\mathbf{On}} V_\alpha$.

Definition

For any set x, we call the **degree** of x ($\deg(x)$) the smallest $\alpha \in \mathbf{On}$ with $x \in \mathbf{V}_\alpha$ (definable).


Next
Grothendieck
Universe
Hereditarily
Finite Sets
∅

Cardinals

Remember, even $\omega^{\omega^{\cdot^{\cdot^{\cdot}}}} = \varepsilon_0$ is countable; but we know uncountable sets exist:

Theorem (Cantor's Theorem)

For any set x, there is no bijective function $f : x \to \mathcal{P}(x)$

Also, by Zermelo's well-ordering theorem, even uncountable sets are well-orderable, and those well-orders are isomorphic to some ordinal number.
$\Rightarrow$ there are uncountable ordinals

Definition

- We call an ordinal α a **cardinal number**, if there is no $\beta < \alpha$ such that there exists a bijection $\beta \to \alpha$.
- Let x be any set. We call the (uniquely determined!) cardinal number $|x|$ such that there is a bijection $x \to |x|$ the **cardinality** of x.

The Cardinal Hierarchy

Definition ($\aleph$)

- $\aleph_0 := \omega$
- For any ordinal α, let $\aleph_{\alpha+1}$ be the smallest cardinal number strictly larger than $\aleph_\alpha$
- For any limit ordinal λ, let $\aleph_\lambda := \bigcup_{\alpha<\lambda} \aleph_\alpha$

We know $|\mathbb{R}| = |\mathcal{P}(\omega)| =: 2^{\aleph_0}$ and $2^{\aleph_0} > \aleph_0$ - but how big is $2^{\aleph_0}$ (or $\aleph_1$, for that matter)?

Definition (The Continuum Hypothesis)

The **Continuum Hypothesis** (CH) is the statement that $2^{\aleph_0} = \aleph_1$.
The **Generalized Continuum Hypothesis** is the statement that $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for every $\alpha \in$ **On**.

Theorem (Cohen, 1963)

Both CH and GCH are neither provable nor disprovable from ZFC

First-order Syntax in ZFC

- A (constant, function or relation) symbol is some/any set. A variable is some/any set. Let F_i, R_i be the sets of function/relation symbols of arity i and V the set of variables.
- A term is a finite sequence of symbols that obeys the recursive definition of a term, hence a set.
- A proposition is a finite sequence of symbols that obeys the recursive definition of a proposition, hence a set.

$\Rightarrow$ The relation $\texttt{IsTerm}_{V,F_0,F_1,\ldots,F_n}(x)$ is definable in ZFC; and hence the set $T := T_{V,F_0,F_1,\ldots,F_n}$ of all terms over $V, F_0, \ldots$.
$\Rightarrow$ the relation $\texttt{IsProposition}_{T,R_1,\ldots,R_m}(x)$ is definable in ZFC; and hence the set $\texttt{Prop}$ of all propositions over $T, R_1, \ldots R_m$.

Proof Theory in ZFC

Let S be a set of axioms (i.e. propositions). A proof rule is a relation $R \subseteq \texttt{Prop}^n \times \texttt{Prop}$. A calculus C is a set of proof rules. We can define the provability relation:

Definition

A sequence of propositions $p = \langle \varphi_1, \ldots, \varphi_n \rangle$ is a C-**proof** iff for each φ_i:

- Either $\varphi_i \in S$ or
- there is some $R \in C$ with $R \subseteq \texttt{Prop}^m \times \texttt{Prop}$ and $\varphi_{j_1}, \ldots \varphi_{j_m}$ such that each $j_k < i$ and $\langle \varphi_{j_1}, \ldots, \varphi_{j_m}, \varphi_i \rangle \in R$.

We say φ is C-**provable from** S (and write $S \vdash_C \varphi$) iff there is some C-proof $p = \langle \varphi_1, \ldots, \varphi_n \rangle$ such that $\varphi_n = \varphi$.

$\Rightarrow$ we can talk about the provability of propositions in ZFC!

Model Theory

Semantics is rather straight-forward – The definition of a model is already based on sets: functions and relations are sets, hence models are sets. The relation $M \vDash \varphi$ is definable (using the usual recursive definition), as is the relation $M \vdash_C \varphi$, hence the completeness theorem becomes a theorem of ZFC!

Theorem (Compactness Theorem)

A set of propositions S has a model iff every finite subset of S has a model

Example

Let c a new constant and extend PA by the axioms
$c \neq 0, c \neq 1, c \neq 2, \ldots$.
$\Rightarrow$ PA has non-standard models.
Every set of propositions that has arbitrarily large finite models has an infinite model.

Even worse:

Theorem (Löwenheim-Skolem)

If a set of propositions S has an infinite model, then it has a model in every infinite cardinality

Example

There are uncountable models of PA. There are countable models of the theory of real numbers.

Theorem (Tarski's Paradox)

If there is a model of ZFC (by Completeness: If ZFC is not contradictory), then there is a countable model of ZFC

$\Rightarrow$ We can not uniquely describe infinite models using the semantics of first-order logic!
(Next best thing: κ-categoricity)

Requirements for Proof Theory

Note that for "embedding" syntax and proof theory in ZFC, all we need is:

- "Encodings" for all symbols (as sets)
- "Encodings" for finite sequences of sets (as sets) such that
- the definitions of "term", "proposition" and "proof" can be expressed (on the basis of sets).

$\Rightarrow$ We don't need "full" sets for that – e.g. natural numbers are already sufficient!

Encoding Sequences as Numbers

Definition

Let $\mathbb{P} = \{p_0, p_1, \ldots\}$ the set of prime numbers and $s = \langle s_0, \ldots, s_n \rangle \in \mathbb{N}^n$ a finite sequence of numbers. The **Gödel number** of s is the number

$$\ulcorner s \urcorner := \prod_{i=0}^{n} p_i^{s_i}$$

By the uniqueness of prime factor decompositions, for any Gödel number n we can obtain the original unique sequence s with $n = \ulcorner s \urcorner$ (i.e. $\ulcorner \cdot \urcorner$ is injective).

Gödelization

Definition

- Let P any recursively enumerable superset of the Peano axioms (with countably many additional symbols).
- For any symbol σ, let $\ulcorner\sigma\urcorner \in \mathbb{N}$ any (unique!) number.
- For any proposition (with free variables) $\varphi = \sigma_0 \dots \sigma_n$, let $\ulcorner\varphi\urcorner := \ulcorner\langle\ulcorner\sigma_0\urcorner, \dots, \ulcorner\sigma_n\urcorner\rangle\urcorner$.
- For any sequence of propositions $p = \langle\varphi_1, \dots, \varphi_n\rangle$, let $\ulcorner p\urcorner := \ulcorner\langle\ulcorner\varphi_1\urcorner, \dots, \ulcorner\varphi_n\urcorner\rangle\urcorner$

Theorem

- *The property* $\texttt{IsProposition}(n)$ *stating that* n *is the Gödel number of a well-formed proposition is definable in* P.
- *The property* $\texttt{IsProof}(p, n)$ *that* p *is a Gödel number of a proof from* P *of the proposition with Gödel number* n *is definable in* P. *Hence, the predicate* $\texttt{Prov}(x) := \exists p\, \texttt{IsProof}(p, x)$ *is definable in* P.

Theorem (Loeb Axioms)

L1 *If* $P \vdash \varphi$, *then* $P \vdash \texttt{Prov}(\ulcorner \varphi \urcorner)$

L2 *If* $P \vdash \texttt{Prov}(\ulcorner \varphi \urcorner) \wedge \texttt{Prov}(\ulcorner \varphi \Rightarrow \psi \urcorner)$, *then* $P \vdash \texttt{Prov}(\ulcorner \psi \urcorner)$

L3 *If* $P \vdash \texttt{Prov}(\ulcorner \varphi \urcorner)$, *then* $P \vdash \texttt{Prov}(\ulcorner \texttt{Prov}(\ulcorner \varphi \urcorner) \urcorner)$

L4 *If* $P \vdash \varphi \Rightarrow \psi$, *then* $P \vdash \texttt{Prov}(\ulcorner \varphi \urcorner) \Rightarrow \texttt{Prov}(\ulcorner \psi \urcorner)$

The Gödel Sentence

Definition (Gödel Sentence)

- Let $\mathtt{sub} : \mathbb{N}^2 \to \mathbb{N}$ the function such that $\mathtt{sub}(\ulcorner\varphi(x)\urcorner, n) = \ulcorner\varphi(n)\urcorner$. Then $\mathtt{sub}$ is definable in P.
- Define the proposition $G(x) := \neg\mathtt{Prov}(\mathtt{sub}(x, x))$ and $\mathcal{G} := G(\ulcorner G(x)\urcorner)$

Then:

$$\mathcal{G} = G(\ulcorner G(x)\urcorner) = \neg\mathtt{Prov}(\ulcorner G(\ulcorner G(x)\urcorner)\urcorner) = \neg\mathtt{Prov}(\ulcorner\mathcal{G}\urcorner)$$

We constructed a sentence that asserts its own non-provability!

Definition

We define the proposition $\mathtt{Con}_P := \neg\mathtt{Prov}(\ulcorner 0 \neq 0 \urcorner)$ expressing that P is consistent.

Theorem (Gödel's Incompleteness Theorems)

1. *P is either inconsistent or incomplete, i.e. there is some sentence φ such that $P \nvdash \varphi$ and $P \nvdash \neg\varphi$.*
2. *If P is consistent, then $P \nvdash \mathtt{Con}_P$.*

The existence of ω proves (in ZFC) that *PA* has a model and hence is consistent; however, we can do the same proof for *ZFC* as with every other sufficiently powerful set of axioms.
$\Rightarrow$ Every plausible foundation for Mathematics is subject to Gödel's theorems!

Non-standard Proofs

If $\mathtt{P} \vdash \mathcal{G}$, then by Loeb $\mathtt{P} \vdash \mathtt{Prov}(\ulcorner \mathcal{G} \urcorner)$ and $\mathtt{P} \vdash \neg\mathtt{Prov}(\ulcorner \mathcal{G} \urcorner)$, contradiction.
But $\mathtt{P} \vdash \neg\mathcal{G} \equiv \mathtt{Prov}(\ulcorner \mathcal{G} \urcorner)$ does not imply $\mathtt{P} \vdash \mathcal{G}$ outright.

- $\Rightarrow$ The Gödel number of the proof could be a non-standard number.
  $\Rightarrow$ have an "infinite" prime factor decomposition, encode an "infinitely long" proof.
- $\Rightarrow$ In ZFC: The set of proofs contains "infinite" elements that are all (in ZFC) provably finite $\Rightarrow$ a non-standard number in ω
- $\Rightarrow$ If $\mathtt{P} \vdash \neg\mathcal{G}$, then no **standard models** can exist (ω-incosistency)

Gödel's Constructible Universe

What's the "smallest" class of sets we could want in ZF (excluding "non-standard" or otherwise "uncomputable" sets)?

Definition

For any set X, we let $\mathtt{Def}(X) :=$
$\{\{y \in X | (X, \in) \vDash \varphi(y)\} | \varphi$ is a predicate defined over $X\} \subseteq \mathcal{P}(X)$
Let $\mathbf{L}_0 := \varnothing$, $\mathbf{L}_{\alpha+1} := \mathtt{Def}(L_\alpha)$ and $\mathbf{L}_\lambda := \bigcup_{\alpha<\lambda} \mathbf{L}_\alpha$ and $\mathbf{L} := \bigcup_{\alpha \in \mathbf{On}} \mathbf{L}_\alpha$.

In ZF, $\mathbf{L}$ is a model of ZFC+GCH.
$\Rightarrow$ If ZF is consistent, then so is ZFC+GCH!
$\Rightarrow$ We need to "add" undefinable (and hence uncomputable) and "unnecessary" sets to make either of them false. (Cohen 1963 "Forcing": we can "adjoin" sets to an existing (inner, countable) universe of sets.)
Fun fact: $\mathbf{L}$ is even definably well-orderable from within $\mathbf{L}$.

Cofinality

$\aleph_0$ is defined as $:= \omega$, but natural numbers are also cardinal numbers. If we let $\aleph'_0 := 0$, then $\aleph'_\omega = \omega$ (Note that $\aleph'_\alpha = \aleph_\alpha$ for $\alpha \geq \omega^2$).
Does the $\aleph$-function have (more) fixed points? i.e. is there a cardinal $\kappa > \omega$ such that $\aleph_\kappa = \kappa$? How could we find/reach/construct such a cardinal?

Definition

- A subset $A \subseteq X$ with X well-ordered is called **cofinite** in X, if for every $x \in X$ there is some $a \in A$ with $x \leq a$.
- Equivalently on cardinals: A subset $A \subseteq \aleph_\alpha$ is called **cofinite** in $\aleph_\alpha$, if $\aleph_\alpha = \bigcup A$.
- The **cofinality** of a (ordinal/) cardinal κ is the smallest (ordinal/) cardinality $\mathtt{cf}(\kappa)$ such that there is some $A \subseteq \kappa$ with A cofinite in κ and (A is well-ordered by $\mathtt{cf}(A)$ /) $|A| = \mathtt{cf}(\kappa)$.

Cofinality $\cong$ "How many smaller (ordinals/) cardinals do I need to construct/approach κ from below?"

Definition

A cardinal number κ is called **singular**, if $\mathtt{cf}(\kappa) < \kappa$ and **regular** if $\mathtt{cf}(\kappa) = \kappa$.

Example

- Every successor ordinal has cofinality 1.
- Every successor cardinal is regular (the union of at most κ many sets with cardinality at most κ is at most $\kappa \cdot \kappa = \kappa$).
- If $\aleph_\lambda$ is a limit cardinal, then $\aleph_\lambda = \bigcup\{\aleph_i \mid i \leq \lambda\}$, hence $\mathtt{cf}(\aleph_\lambda) \leq |\lambda|$, hence $\aleph_\lambda$ is singular, if not a fixed point.

$\Rightarrow$ If $\aleph_\kappa = \kappa$, then κ is a regular limit cardinal, and conversely.

Large Cardinals

So are there regular limit cardinals?

Definition

- A (uncountable) regular limit cardinal is called **(weakly) inaccessible**.
- A weakly inaccessible cardinal κ such that $2^\alpha < \kappa$ for all $\alpha < \kappa$ is called **strongly inaccessible** (under GCH equivalent).

Theorem

- *If $\kappa > \omega$ is weakly inaccessible, then $\mathbf{L}_\kappa \vDash ZFC$.*
- *If $\kappa > \omega$ is strongly inaccessible, then $\mathbf{V}_\kappa \vDash ZF$.*

$\Rightarrow$ *by the second incompleteness theorem, the existence of inaccessible cardinals is unprovable.*

In ZFC, the statement $\mathtt{Con}_{\mathtt{ZFC}}$ is "almost equivalent" to the existence of an inaccessible cardinal.

Grothendieck Universes

Are large cardinals reasonable?

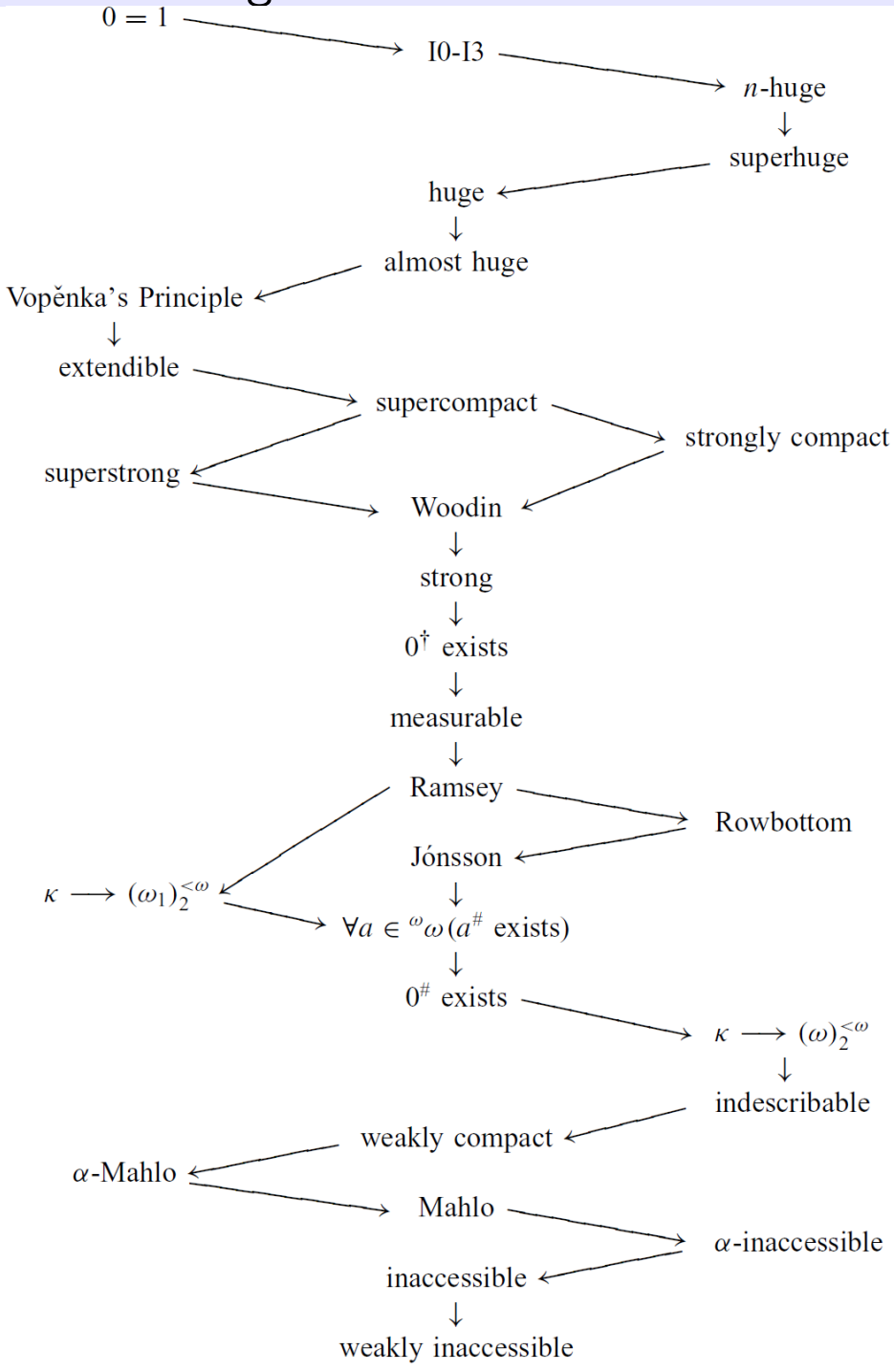
Note: The axiom of Infinity posits an "inaccessible" cardinal!

- $\mathbf{V}_\omega \vDash ZFC^{FIN}$
- ω is a regular limit cardinal
- If $\aleph'_0 := 0$, then $\aleph'_\omega = \omega$ is a fixed point

$\Rightarrow$ The jump from "normal" sets to large cardinals is "equivalent" to the jump from finite sets to infinite sets ("strong infinity axioms")

Definition

- A set U is called **Grothendieck Universe**, if U is transitive and closed under pair sets, powersets and unions.
- The Grothendieck axiom states that every set lives in a Grothendieck universe.


0 = 1
I0-I3
n-huge
superhuge
huge
almost huge
Vopěnka's Principle
extendible
supercompact
strongly compact
superstrong
Woodin
strong
0† exists
measurable
Ramsey
Rowbottom
Jónsson
κ ⟶ (ω1)2<ω
∀a ∈ ω ω (a# exists)
0# exists
κ ⟶ (ω)2<ω
indescribable
weakly compact
α-Mahlo
Mahlo
α-inaccessible
inaccessible
weakly inaccessible