Large cardinals in mathematics and infinite combinatorics

Vincenzo Dimonte

20 April 2016

A point of view: the development of mathematics is driven by a search for completion.

The integers are developed for completing the natural numbers under substraction.

The rationals are developed for completing the integers under division.

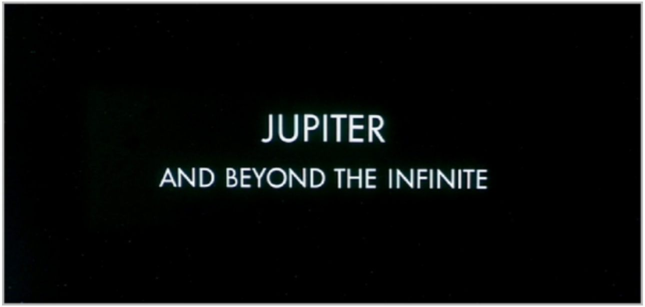
The reals are developed for completing the rationals under Cauchy sequences.

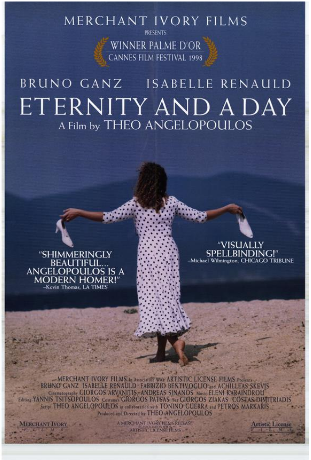
The complex numbers are developed for completing the reals under square roots.

What about counting?

$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad \ldots \quad \infty \; \infty + 1$

SPACE RANGER
LIGHTYEAR


JUPITER
AND BEYOND THE INFINITE


MERCHANT IVORY FILMS
PRESENTS
WINNER PALME D'OR
CANNES FILM FESTIVAL 1998
BRUNO GANZ ISABELLE RENAULD
ETERNITY AND A DAY
A Film by THEO ANGELOPOULOS
"SHIMMERINGLY BEAUTIFUL... ANGELOPOULOS IS A MODERN HOMER!"
–Kevin Thomas, LA TIMES
"VISUALLY SPELLBINDING!"
–Michael Wilmington, CHICAGO TRIBUNE
MERCHANT IVORY FILMS In Association With ARTISTIC LICENSE FILMS Presents
BRUNO GANZ ISABELLE RENAULD FABRIZIO BENTIVOGLIO and ACHILLEAS SKEVIS
Cinematography GIORGOS ARVANITIS - ANDREAS SINANOS Music ELENI KARAINDROU
Editing YANNIS TSITSOPOULOS Costumes GIORGOS PATSAS Set GIORGOS ZIAKAS COSTAS DIMITRIADIS
Script THEO ANGELOPOULOS in collaboration with TONINO GUERRA and PETROS MARKARIS
Produced and Directed by THEO ANGELOPOULOS
MERCHANT IVORY FILMS
A MERCHANT IVORY FILMS RELEASE IN ASSOCIATION WITH ARTISTIC LICENSE FILMS
Artistic License FILMS

JUNO REACTOR
BEYOND THE INFINITE

There are some psychological studies that indicates that the concept of "infinity plus one" is natural for children

Monaghan, John (2001). "Young Peoples' Ideas of Infinity". *Educational Studies in Mathematics* **48** (2): 239–257

In mathematics: uniqueness of an expansion of a function in a trigonometric series.

Theorem (Cantor, 1870)

Suppose

$$a_0/2 + \sum_{n=1}^{+\infty} (a_n \cos nx + b_n \sin nx) = 0 \text{ for any } x \in \mathbb{R}.$$

Then $a_n = b_n = 0$.

In trying to extend this results (weakening the hypothesis from $\forall x$), Cantor arrived to this definition:

Definition (Cantor, 1872)

Let S be a set of reals. Then $S' = \{x \in S : x \text{ is a limit point of } S\}$. Define by induction:

- $S^{(0)} = S'$;
- $S^{(n+1)} = S^{(n)'}$;
- $S^{(\infty)} = \bigcap_{n \in \mathbb{N}} S^{(n)}$.

But maybe $S^{(\infty)}$ has some isolated points...

- $S^{(\infty+1)} = S^{(\infty)'} \ldots$

Definition (Cantor, 1883)

Two ordered sets $(S, \leq_S)$ and $(T, \leq_T)$ have the same *order type* if there is an order isomorphism between them, i.e., $\exists f : S \to T$ bijective such that $x \leq_S y$ iff $f(x) \leq_T f(y)$.

α is an *ordinal number* if it's the order type of a well-ordered set (i.e., linear without infinite descending chains).

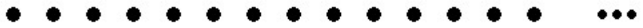
1

● ●

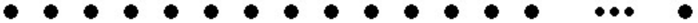
2

3

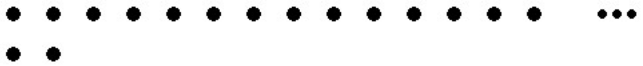
$$\infty$$



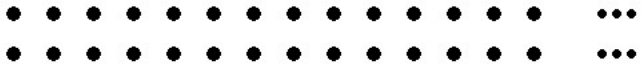
ω



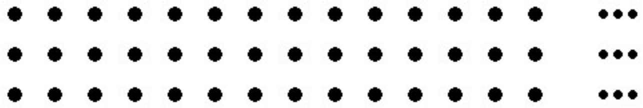
$\omega + 1$



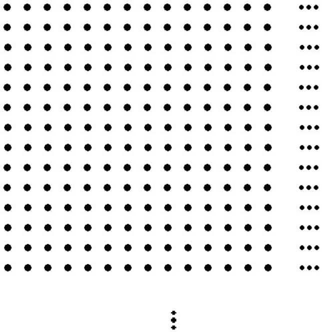
$$\omega + 2$$



$$\omega + \omega = \omega \cdot 2$$

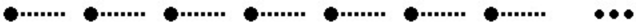


$$\omega + \omega + \omega = \omega \cdot 3$$



$\omega \cdot \omega$

(the order type of the Sieve of Eratosthenes)



$$\omega \cdot \omega$$

But wait a minute...

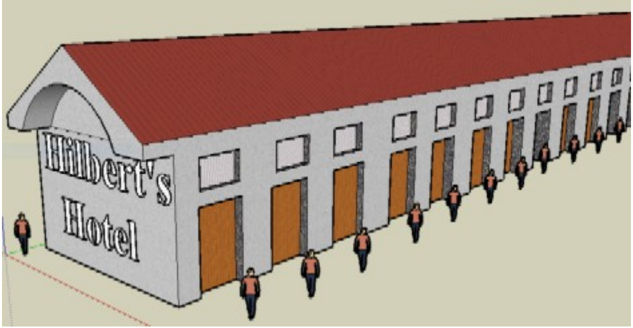
$\omega + 1$ is after ω, but it's not bigger!

Definition(Cantor, 1874-1884)

Two sets have the same *cardinality* if there is a bijection between them.
κ is a *cardinal number* if it is the cardinality of an ordinal number.

ω is both a cardinal and an ordinal number. When we use it as a cardinal, we call it $\aleph_0$.

There is a bijection between $\omega + 1$ and ω (Hilbert's Paradox of the Grand Hotel). Is there an ordinal really bigger?


Hilbert's
Hotel

Galileo's paradox

⋮	⋮
7	
6	6
5	
4	4
3	
2	2
1	

Galileo's paradox

⋮	⋮
7	14
6	12
5	10
4	8
3	6
2	4
1	2

Theorem(Cantor, 1874)

$|\mathcal{P}(\omega)| > \aleph_0$.

Identify a subset of ω as an ω-sequence of 0's and 1's.

$$\begin{array}{cccccccccccccc}
1 & \to & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \dots \\
2 & \to & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\
3 & \to & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \dots \\
4 & \to & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & \dots \\
5 & \to & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & \dots \\
6 & \to & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & \dots \\
7 & \to & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\
8 & \to & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & \dots \\
9 & \to & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & \dots \\
10 & \to & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & \dots \\
11 & \to & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \dots \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \dots
\end{array}$$

Theorem(Cantor, 1874)

$|\mathcal{P}(\omega)| > \aleph_0$.

Identify a subset of ω as an ω-sequence of 0's and 1's.

1	$\to$	0	0	1	1	0	1	0	1	0	1	0	$\dots$
2	$\to$	0	1	1	1	1	0	0	0	0	0	0	$\dots$
3	$\to$	0	1	0	0	0	0	1	0	0	0	0	$\dots$
4	$\to$	1	1	1	1	1	0	0	1	1	1	0	$\dots$
5	$\to$	0	1	0	1	0	0	1	0	1	0	1	$\dots$
6	$\to$	0	0	1	1	0	1	1	0	1	1	1	$\dots$
7	$\to$	1	0	0	0	1	1	1	1	1	1	1	$\dots$
8	$\to$	0	1	1	0	1	0	1	0	0	1	1	$\dots$
9	$\to$	0	1	0	1	1	1	0	0	1	1	0	$\dots$
10	$\to$	1	1	1	0	0	1	1	1	1	1	0	$\dots$
11	$\to$	1	1	0	0	0	1	0	0	0	0	0	$\dots$
$\vdots$		$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$
		1	0	1	0	1	0	0	1	0	0	1	$\dots$

The smallest cardinal bigger than $\aleph_0$ is $\aleph_1$, then $\aleph_2$, $\aleph_3$, $\ldots \aleph_\omega$, $\aleph_{\omega+1}$, $\ldots \aleph_{\omega^\omega}$ $\ldots$

Operations are defined, like sum, multiplications...

Definition

$\kappa^\gamma = |\{f : \gamma \to \kappa\}|$.

For example $2^\kappa = |\mathcal{P}(\kappa)|$.

Main Problems in Set Theory #2

Suppose for any n, $2^{\aleph_n} < \aleph_\omega$. How big is $2^{\aleph_\omega}$?
Best result: $2^{\aleph_\omega} < \aleph_{\omega_4}$.

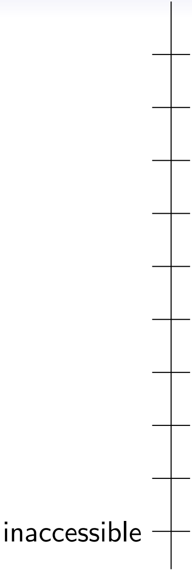
But wait a minute...

$\aleph_1$ is still too close to $\aleph_0$: $2^{\aleph_0} \geq \aleph_1$, but $2^n < \aleph_0$ for all n!

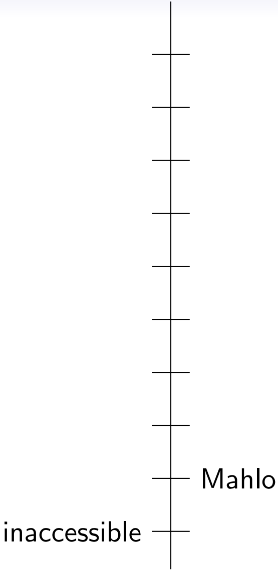
Definition(Sierpiński, Tarski, Zermelo, 1930)

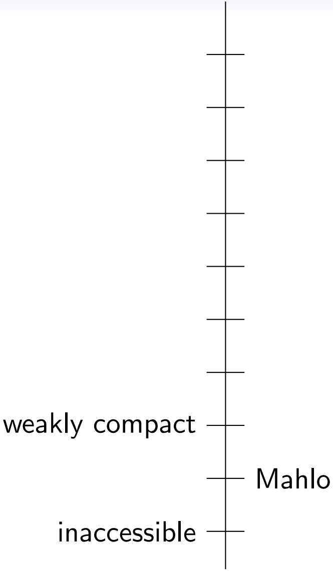
κ is an inaccessible cardinal iff

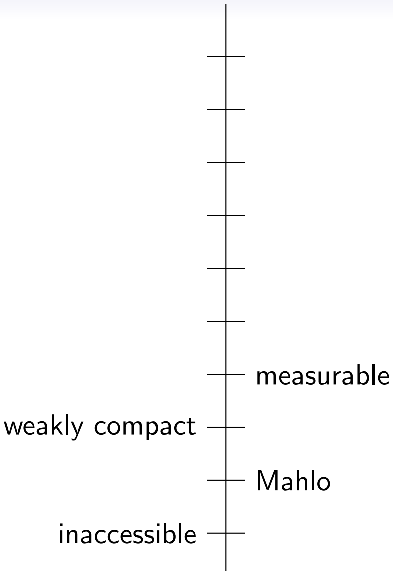
- $\kappa > \aleph_0$;
- for any $\gamma, \eta < \kappa$, $\gamma^\eta < \kappa$;
- for any $A \subseteq \kappa$, $|A| < \kappa \to \sup(A) < \kappa$.

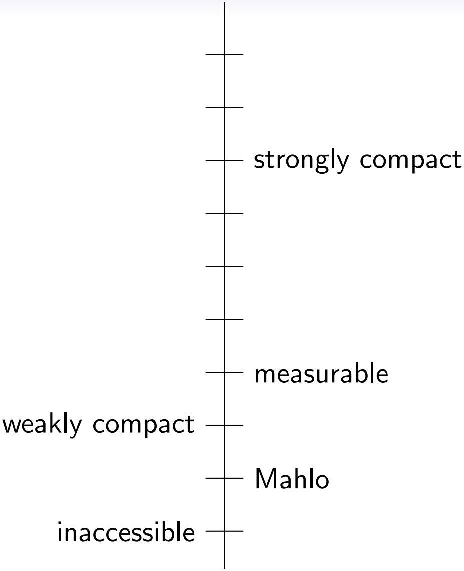


inaccessible


Mahlo
inaccessible


weakly compact
Mahlo
inaccessible


measurable
weakly compact
Mahlo
inaccessible


strongly compact
measurable
weakly compact
Mahlo
inaccessible

Mathematics works through *theorems*.

They are logical derivations of the form if. . . then. . . .

It is clear that there needs to be a starting point, i.e., an axiomatic system.

ZFC is now the favourite axiomatic system for mathematics. We can say it's *the* mathematics.

Theorem(Gödel, 1931)

Any effectively generated theory capable of expressing elementary arithmetic cannot be both consistent and complete.

For any formal effectively generated theory T including basic arithmetical truths and also certain truths about formal provability, if T includes a statement of its own consistency then T is inconsistent.

A statement is *independent from ZFC* if ZFC cannot prove it or disprove it.

If there is an inaccessible cardinal, then one can prove that ZFC is consistent. Then ZFC cannot prove that there exists an inaccessible cardinal, so it's independent from ZFC.

Theorem

The existence of an inaccessible cardinal is equiconsistent to

- the measurability of the projective sets in $\mathbb{R}$;
- the existence of Kurepa trees.

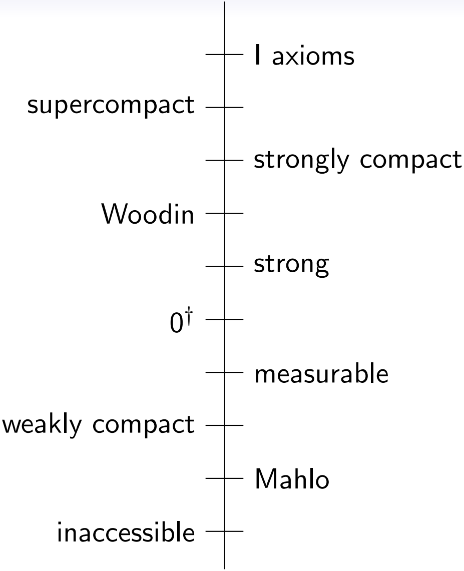
Theorem

The existence of a measurable cardinal is equiconsistent to

- every Borelian measure on $\mathcal{B}([0,1])$ can be extended on a measure on $\mathcal{P}([0,1])$;
- there exists a cardinal κ and a non-trivial homomorphism $h : \mathbb{Z}^\kappa \setminus \mathbb{Z}^{<\kappa} \to \mathbb{Z}$.

Theorem(Nyikos, Fleissner 1982)

The consistency of the normal Moore conjecture is between measurable and strongly compact.



I axioms

supercompact

strongly compact

Woodin

strong

$0^\dagger$

measurable

weakly compact

Mahlo

inaccessible

Theorem (Wiles, 1995)

Suppose there are unboundedly inaccessible cardinals. Then for any $n > 2$ there are no a, b, c integers such that $a^n + b^n = c^n$.

In 1983 Pitowsky constructed hidden variable models for spin-1/2 and spin-1 particles in quantum mechanics. Pitowsky's functions calculate in this model the probabilities of spin values.

Theorem (Farah, Magidor, 2012)

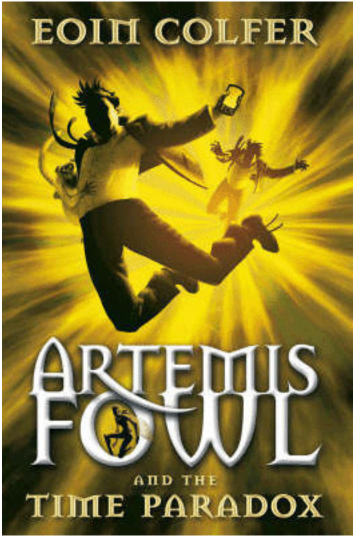
If there exists a measurable cardinal, then Pitowski functions do not exist.

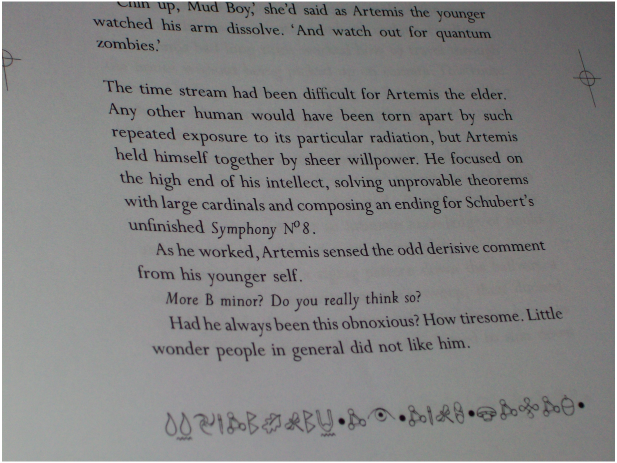
There are also very debatable results. . .

Theorem (H. Friedman, 2012)

The existence of a measurable cardinal is close to equiconsistent to the existence of God.

. . . and large cardinals even appear in pop culture!


EOIN COLFER
ARTEMIS FOWL
AND THE
TIME PARADOX



Chin up, Mud Boy,' she'd said as Artemis the younger watched his arm dissolve. 'And watch out for quantum zombies.'

The time stream had been difficult for Artemis the elder. Any other human would have been torn apart by such repeated exposure to its particular radiation, but Artemis held himself together by sheer willpower. He focused on the high end of his intellect, solving unprovable theorems with large cardinals and composing an ending for Schubert's unfinished *Symphony* N°8.

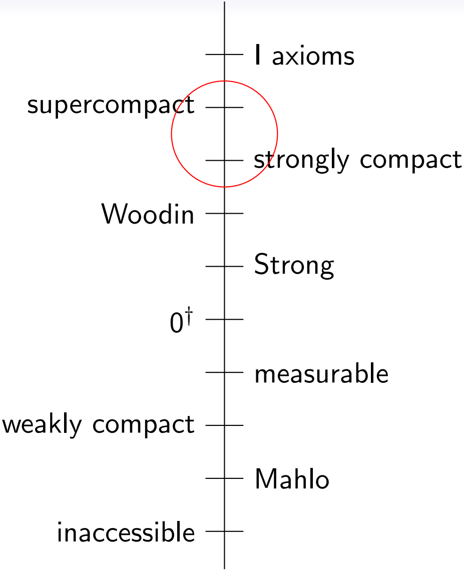
As he worked, Artemis sensed the odd derisive comment from his younger self.

More B minor? Do you really think so?

Had he always been this obnoxious? How tiresome. Little wonder people in general did not like him.

Main questions when dealing with a large cardinal:

- What is the relationship between it and other large cardinals? E.g. is it really different? Is it really stronger (or weaker)?
- What are its consequences on set theory? And mathematics?
- Which theorems *needs* it to be proven?



I axioms

supercompact

strongly compact

Woodin

Strong

$0^\dagger$

measurable

weakly compact

Mahlo

inaccessible

Main Problems in Set Theory #3

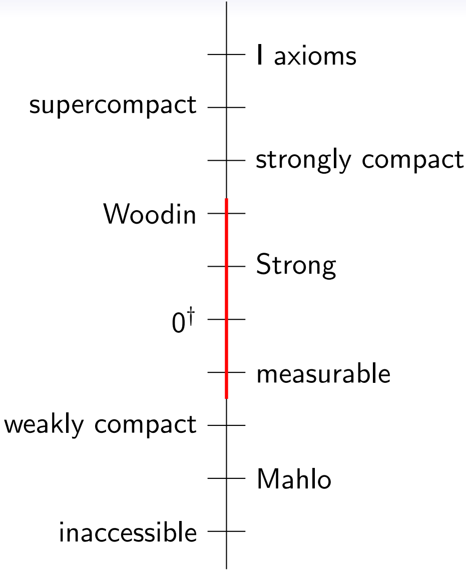
Is supercompact equiconsistent to strongly compact?

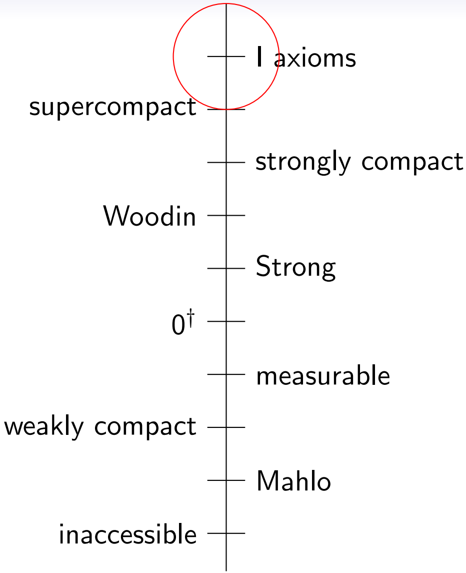
Main Problems in Set Theory #5

Suppose κ is strongly compact. Is it true that if for any $\eta < \kappa$ $2^\eta = \eta^+$, then this is true for every η?

Main Problems in Set Theory #1

Is there an inner model for supercompact?


I axioms
supercompact
strongly compact
Woodin
Strong
$0^\dagger$
measurable
weakly compact
Mahlo
inaccessible



I axioms

supercompact

strongly compact

Woodin

Strong

$0^\dagger$

measurable

weakly compact

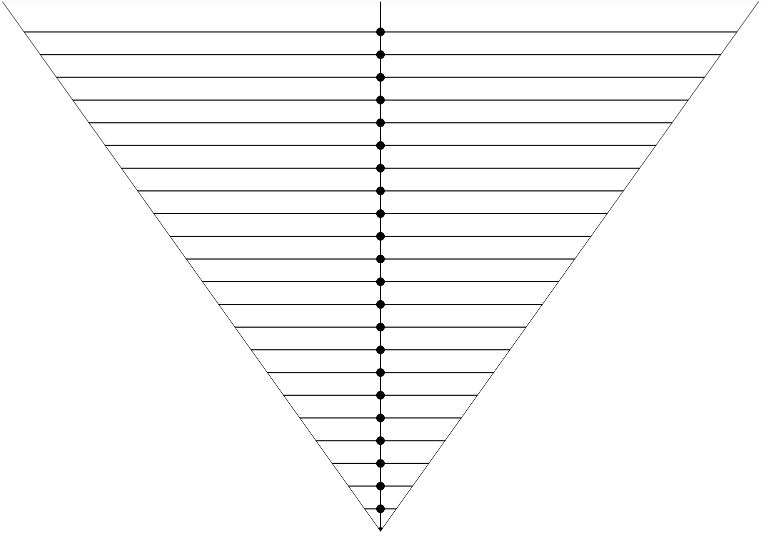
Mahlo

inaccessible

Definition

The rank of $\emptyset$ is 0.The rank of a set S is the supremum of the ranks of all $s \in S$ plus $1. V_\alpha$ is the set of the sets of rank $< \alpha. V = \bigcup_\alpha V_\alpha$ is the universe of sets.

Examples: $V_0 = \emptyset$. $\emptyset \in V_1$, $\{\emptyset\} \in V_2$, $\{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\} \in V_3$, ...



Definition

A function $j : M \to N$ is an *elementary embedding* if it is injective and for any $x \in M$ and any formula φ, $M \vDash \varphi(x)$ iff $N \vDash \varphi(j(x))$. We write $j : M \prec N$.

It's a morphism for the logical structure.

If $x, y \in M$ and $x \in y$, then $j(x) \in j(y)$. If $\exists x \in M$ that satisfies something, then $\exists y \in N$ that satisfies the same thing. If all $x \in M$ satisfy something relative to a parameter p, then all $y \in N$ satisfy the same thing relative to the parameter $j(p)$.

$j(0) = 0,\ j(1) = 1,\ j(2) = 2,\ \dots\ j(n) = n,\ \dots,\ j(\omega) = \omega,\ j(\aleph_\omega) = \aleph_\omega, \dots$

The critical point of j is the smallest ordinal α such that $j(\alpha) \neq \alpha$ (it's easy to see that $j(\alpha) \geq \alpha$).

Theorem (Scott, Keisler 1962)

The following are equivalent:

- there is a κ-additive measure on κ (κ is measurable);
- there exists $j : V \prec M \subseteq V$, with κ critical point of j.

Can $V = M$? It would be a very strong hypothesis...

Theorem (Kunen, 1971)

There is no $j : V \prec V$.

The proof uses greatly the Axiom of Choice.

Main Problems in Set Theory #4

Is there a $j : V \prec V$ when $\neg AC$?.

Let's define a local version of such hypothesis:

Definition

- I3: There exists $j : V_\lambda \prec V_\lambda$;
- I1: There exists $j : V_{\lambda+1} \prec V_{\lambda+1}$.

An example of consequences of very large cardinals: left distributive algebras.

Note: given the limitations of inner model theory, it is not possible (for now) to prove that they are necessary.

Let's start with a symbol, any: x, y, $\spadesuit$, 👩. . .

We add an operation: $\cdot$.

x, $x \cdot x$, $(x \cdot x) \cdot x$, $x \cdot ((x \cdot x) \cdot x)$, $x \cdot (x \cdot (x \cdot (x \cdot x)))$, . . .

We add just one rule (LD): $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot (a \cdot c)$. This is what we call *free* left distributive algebra with one generator.

So for example $x \cdot (x \cdot x) \equiv (x \cdot x) \cdot (x \cdot x) \equiv ((x \cdot x) \cdot x) \cdot ((x \cdot x) \cdot x)$, $x \cdot ((x \cdot x) \cdot x) \equiv (x \cdot (x \cdot x))(x \cdot x)$.

Is there an algorithm that, given two "words", tells you whether they are equivalent or not?

Theorem (Laver, 1989)

Under I3, the word problem for LD-algebras is decidable.

The main idea behind it is that the set of embeddings in V_λ is a free LD algebra... and there is just one! The second idea is defining a division algorithm and proving that strict division is irreflexive.

Theorem (Dehornoy, 1994)

The word problem for LD-algebras is decidable.

Laver tables:

Suppose we want our LD-algebras to be *finite*. We consider $\{1, \ldots, N\}$ as generators. We have two rules:

- $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot (a \cdot c)$
- $a \cdot 1 \equiv a + 1$ (where $+$ is cyclical).

We call such algebra S_N.

Theorem

- S_N, when it exists, is unique;
- S_N exists iff $N = 2^n$ for some $n \in \mathbb{N}$ (we call it A_n);
- for any a, the orbit of a under $\cdot$ is periodical.

A_2	1	2	3	4
1				
2				
3				
4				

A_2	1	2	3	4
1	2			
2	3			
3	4			
4	1			

A_2	1	2	3	4
1	2			
2	3			
3	4			
4	1	2		

$$4 \cdot 2 = 4 \cdot (1 \cdot 1) = (4 \cdot 1) \cdot (4 \cdot 1) = 1 \cdot 1 = 2$$

A_2	1	2	3	4
1	2			
2	3			
3	4			
4	1	2	3	4

$$4 \cdot 3 = 4 \cdot (2 \cdot 1) = (4 \cdot 2) \cdot (4 \cdot 1) = 2 \cdot 1 = 3$$
$$4 \cdot 4 = 4 \cdot (3 \cdot 1) = (4 \cdot 3) \cdot (4 \cdot 1) = 3 \cdot 1 = 4$$

A_2	1	2	3	4
1	2			
2	3			
3	4	4	4	
4	1	2	3	4

$$3 \cdot 2 = 3 \cdot (1 \cdot 1) = (3 \cdot 1) \cdot (3 \cdot 1) = 4 \cdot 4 = 4$$
$$3 \cdot 3 = 3 \cdot (2 \cdot 1) = (3 \cdot 2) \cdot (3 \cdot 1) = 4 \cdot 4 = 4$$

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

A_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	12	14	16	2	12	14	16	2	12	14	16	2	12	14	16
2	3	12	15	16	3	12	15	16	3	12	15	16	3	12	15	16
3	4	8	12	16	4	8	12	16	4	8	12	16	4	8	12	16
4	5	6	7	8	13	14	15	16	5	6	7	8	13	14	15	16
5	6	8	14	16	6	8	14	16	6	8	14	16	6	8	14	16
6	7	8	15	16	7	8	15	16	7	8	15	16	7	8	15	16
7	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	16
8	9	10	11	12	13	14	15	16	9	10	11	12	13	14	15	16
9	10	12	14	16	10	12	14	16	10	12	14	16	10	12	14	16
10	11	12	15	16	11	12	15	16	11	12	15	16	11	12	15	16
11	12	16	12	16	12	16	12	16	12	16	12	16	12	16	12	16
12	13	14	15	16	13	14	15	16	13	14	15	16	13	14	15	16
13	14	16	14	16	14	16	14	16	14	16	14	16	14	16	14	16
14	15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Can we say something about the periods?

- Is there a relation between periods for different rows in the same table?
- Given n, is there a row in some table with period n?
- If so, how big is the table?

Theorem (Laver, 1995)

Under I3,

- for every $n \in \mathbb{N}$, the period of the second row of A_n is $\geq$ the period of the first row of A_n
- for every $p \in \mathbb{N}$, there exist n such that the first row of A_n has period 2^p.

There is no known proof of this that does not use large cardinals.

It is not possible in primitive recursive arithmetic:

Theorem (Dougherty)

Let $q(p)$ the minimal n such that the first row of A_n has period 2^p. Then $q(0) = 0$, $q(1) = 2$, $q(2) = 3$, $q(3) = 5$, $q(4) = 9$, $q(5) > f_9(f_8(f_8(254)))$, where f is the Ackermann function.

To recap:

- Completing the natural numbers under the operation of "‘counting"’, opens up a very rich universe;
- large cardinal are seemingly innocuous infinite combinatorial properties;
- yet they function very well as a measure for calculating the strength of many mathematical propositions;
- for unknown reason, they are ordered in a linear way;
- large cardinals above Woodin are more misterious, because we don’t have inner model theory there;
- yet they are also the more potentially productive.

Thanks for your attention!

Twitter: @DimonteSet
Blog: cantorontheshore.blogspot.com
Youtube: see Vsauce video "'How to count past infinity"'.