INFTY @ ESSLLI 2011

Scientific and Financial Report

The INFTY Steering Committee had decided in Vienna (February 2010) that INFTY should show some presence at the *European Summer School for Logic, Language and Information* ESSLLI. INFTY@ESSLLI2011 was the first such event and will be followed by INFTY@ESSLLI 2012.

We see these events as an important step towards re-injecting mathematical logic into the programme of the ESSLLI schools: In recent years, ESSLLI has seen a shift from foundational studies to less mathematical courses and workshops. Several ESSLLIs had so little mathematical content that it was not useful for PhD students in mathematical logic to attend this otherwise very important networking event. It is in the interest of the mathematical logic community that these summer schools remain interesting for students working in the foundations of mathematics; furthermore, it is of interest for us to make sure that mathematical logic remains an important part of the community represented at ESSLLI.

Together with Mirna Dzamonja and Grzegorz Plebenek, the applicant coordinated a course and a workshop at ESSLLI 2011. Course and workshop proposal were accepted by the programme committee of ESSLLI on 10 June 2010.

The course (level: foundational course) was entitled *Basic set-theoretic techniques in logic* and was taught by Benedikt Löwe & Grzegorz Plebanek on five consecutive days. The slides of this course are online at

`http://www.math.uni-hamburg.de/home/loewe/INFTY@ESSLLI2011/course.html`

and attached to this report (103 pages).

Many participants of ESSLLI do not have a mathematical background, and most set theory courses are aimed at mathematicians and thus tend to be inaccessible to non-mathematicians. However, the basic techniques of set theory are important well beyond mathematical logic and should be known to all logicians. In our foundational course, we offered an introduction to these for a broad audience.

The workshop, organized by Mirna Dzamonja and the applicant had xx talks, among them three tutorials aimed at students. The following is the schedule of the workshop:

Monday, 1 August 2011

14:00-14:30	*Tutorial 1.1: Combinatorial Set Theory* Jean Larson. *University of Florida, U.S.A.*
14:30-15:00	*Tutorial 2.1: Descriptive Set Theory* Martin Goldstern. *Technische Universität Wien, Austria.*
15:00-15:30	*Classification in descriptive set theory* Alberto Marcone. *Università di Udine, Italy.*

Tuesday, 2 August 2011

14:00-14:30	*Tutorial 3.1: Forcing* Gregor Dolinar. *Univerza v Ljubljani, Slovenia.*
14:30-15:00	*Tutorial 1.2: Combinatorial Set Theory* Jean Larson. *University of Florida, U.S.A.*
15:00-15:30	*Blass's game semantics for linear logic without the axioms of choice* Zhenhao Li. *Universiteit van Amsterdam, The Netherlands.*

Wednesday, 3 August 2011

14:00-14:30	*Tutorial 2.2: Descriptive Set Theory* Martin Goldstern. *Technische Universität Wien, Austria.*
14:30-15:00	*Tutorial 3.2: Forcing* Gregor Dolinar. *Univerza v Ljubljani, Slovenia.*
15:00-15:30	*Half-filling families of finite sets* Grzegorz Plebanek. *Uniwersytet Wrocławski, Poland.*

Thursday, 4 August 2011

14:00-14:30	*Tutorial 1.3: Combinatorial Set Theory* Jean Larson. *University of Florida, U.S.A.*
14:30-15:00	*Tutorial 2.3: Descriptive Set Theory* Martin Goldstern. *Technische Universität Wien, Austria.*
15:00-15:30	*MAD families and the projective hierarchy* Yurii Khomskii. *Universiteit van Amsterdam, The Netherlands.*

Friday, 5 August 2011

14:00-14:45	*Tutorial 3.3: Forcing* Gregor Dolinar. *Univerza v Ljubljani, Slovenia.*
14:45-15:30	Discussion

The webpage of the workshop can be found at

`http://www.math.uni-hamburg.de/home/loewe/INFTY@ESSLLI2011/`

The foundational course was very successful with between 20 and 30 students actively participating. The chair of the programme committee of ESSLLI 2012 was present during one of the lectures and informed us that he wanted to have a similar mathematical logic course at the foundational level for ESSLLI 2012 (this will be realized by Bob Lubarsky's course).

While we would also consider the workshop a success, it was rather difficult to get set theorists to submit to the workshop: the original idea was that a larger group of set theorists would create a critical mass. In fact, we had only the invited speakers plus two graduate students. For ESSLLI 2012, we therefore decided not include a workshop component.

Financial Report.

Travel Expenses. We covered the travel expenses of six participants: Mirna Dzamonja (EUR 173), Jean Larson (EUR 694), Zhenhao Li (EUR 300), Benedikt Löwe (EUR 445), Grzegorz Plebanek (EUR 373), and Sourav Tarafder (EUR 440).

Total Travel Expenses. **EUR 2425.**

Accommodation Expenses. We booked and paid hotel rooms in two hotels: the Hotel Pri Mraku and the Hotel Slon. In total we paid for 24 nights for the participants Goldstern, Larson, Löwe, and Plebanek at a rate of approximately 75 EUR a night.

Total Accommodation Expenses. **EUR 1801.**

Meals. The costs of the lecturers' dinner were covered by ESSLLI for the lecturers of the course (Löwe and Plebanek) and the organizer of the workshop. In order to allow more interaction between the invited speakers and the organizers, we covered the costs of the lecturers' dinner for our invited speakers.

Total Meal Costs. **EUR 122.**

Other costs. As discussed in the proposal, we needed to cover registration fees for some of our invited speakers (two fee waivers were given as part of the workshop). We paid EUR 700 in registration fees to the ESSLLI 2011 organizers.

Total Other Costs. **EUR 700.**

Ordinals and Cardinals: Basic set-theoretic techniques in logic

Benedikt Löwe
Universiteit van Amsterdam
Grzegorz Plebanek
Uniwersytet Wrocławski

ESSLLI 2011, Ljubljana, Slovenia

This course is a foundational course (no prerequisites) on basic techniques of set theory. It consists of five lectures (given by BL= 'Benedikt' and GP= 'Grzegorz'):

Programme

Monday	General introduction (BL) *Measuring the infinite: Cardinal numbers* (GP)
Tuesday	*Counting beyond infinity: Ordinal numbers* (GP)
Wednesday	*Transfinite recursion and induction* (BL)
Thursday	*The Axiom of choice* (GP)
Friday	*Set-theoretic analysis of infinite games* (BL)

No exams:-)

This course is a foundational course (no prerequisites) on basic techniques of set theory. It consists of five lectures (given by BL= 'Benedikt' and GP= 'Grzegorz'):

Programme

Monday	General introduction (BL)
	Measuring the infinite: Cardinal numbers (GP)
Tuesday	*Counting beyond infinity: Ordinal numbers* (GP)
Wednesday	*Transfinite recursion and induction* (BL)
Thursday	*The Axiom of choice* (GP)
Friday	*Set-theoretic analysis of infinite games* (BL)

No exams:-)

This course is a foundational course (no prerequisites) on basic techniques of set theory. It consists of five lectures (given by BL= 'Benedikt' and GP= 'Grzegorz'):

Programme

Monday	General introduction (BL) *Measuring the infinite: Cardinal numbers* (GP)
Tuesday	*Counting beyond infinity: Ordinal numbers* (GP)
Wednesday	*Transfinite recursion and induction* (BL)
Thursday	*The Axiom of choice* (GP)
Friday	*Set-theoretic analysis of infinite games* (BL)

No exams:-)

This course is a foundational course (no prerequisites) on basic techniques of set theory. It consists of five lectures (given by BL= 'Benedikt' and GP= 'Grzegorz'):

Programme

Monday	General introduction (BL)
	Measuring the infinite: Cardinal numbers (GP)
Tuesday	*Counting beyond infinity: Ordinal numbers* (GP)
Wednesday	*Transfinite recursion and induction* (BL)
Thursday	*The Axiom of choice* (GP)
Friday	*Set-theoretic analysis of infinite games* (BL)

No exams:-)

This course is a foundational course (no prerequisites) on basic techniques of set theory. It consists of five lectures (given by BL= 'Benedikt' and GP= 'Grzegorz'):

Programme

Monday	General introduction (BL)
	Measuring the infinite: Cardinal numbers (GP)
Tuesday	*Counting beyond infinity: Ordinal numbers* (GP)
Wednesday	*Transfinite recursion and induction* (BL)
Thursday	*The Axiom of choice* (GP)
Friday	*Set-theoretic analysis of infinite games* (BL)

No exams:-)

The two protagonists of set theory.

- Cardinal numbers.

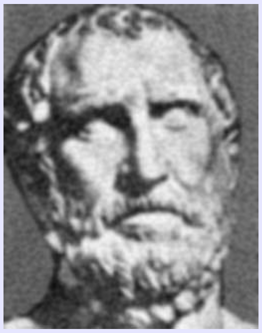
  Measuring the size of infinity and comparing the sizes of infinite sets.

- Ordinal numbers.

  Counting beyond infinity and providing the means of exhausting infinite sets by iterative processes.

Until the 19th century, infinity had been considered to be a rather problematic concept.

Achilles and the tortoise.

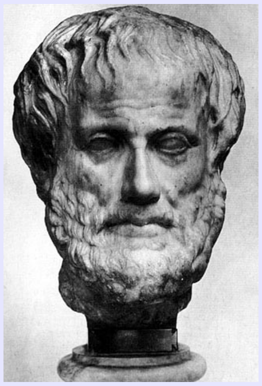


Zeno of Elea, c. 490 BC – c. 430 BC

The argument says that it is impossible for [Achilles] to overtake the tortoise when pursuing it. For in fact it is necessary that what is to overtake [something], before overtaking [it], first reach the limit from which what is fleeing set forth. In [the time in] which what is pursuing arrives at this, what is fleeing will advance a certain interval ... And in the time again in which what is pursuing will traverse this [interval] which what is fleeing advanced, in this time again what is fleeing will traverse some amount ...

Simplicius, On Aristotle's Physics, 1014.10

Aristotle and the Actual Infinite.



Aristotle, 384 BC - 322 BC

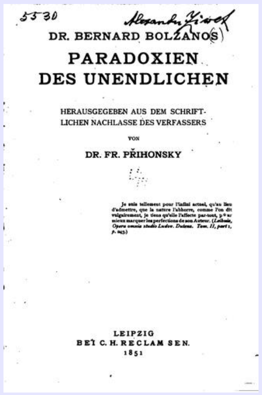
For generally the infinite has this mode of existence: one thing is always being taken after another, and each thing that is taken is always finite, but always different.

Aristotle, Physica, III.6

For the fact that the process of dividing never comes to an end ensures that this activity exists potentially, but not that the infinite exists separately.

Aristotle, Metaphysica, IX.6

Paradoxien des Unendlichen



DR. BERNARD BOLZANO'S

PARADOXIEN DES UNENDLICHEN

HERAUSGEGEBEN AUS DEM SCHRIFTLICHEN NACHLASSE DES VERFASSERS

VON

DR. FR. PŘIHONSKY

LEIPZIG
BEI C. H. RECLAM SEN.
1851

Bernard Bolzano, 1781–1848

§18 Nicht eine jede Größe, die wir als Summe einer unendlichen Menge anderer, die alle endlich sind, ist selbst eine unendliche.

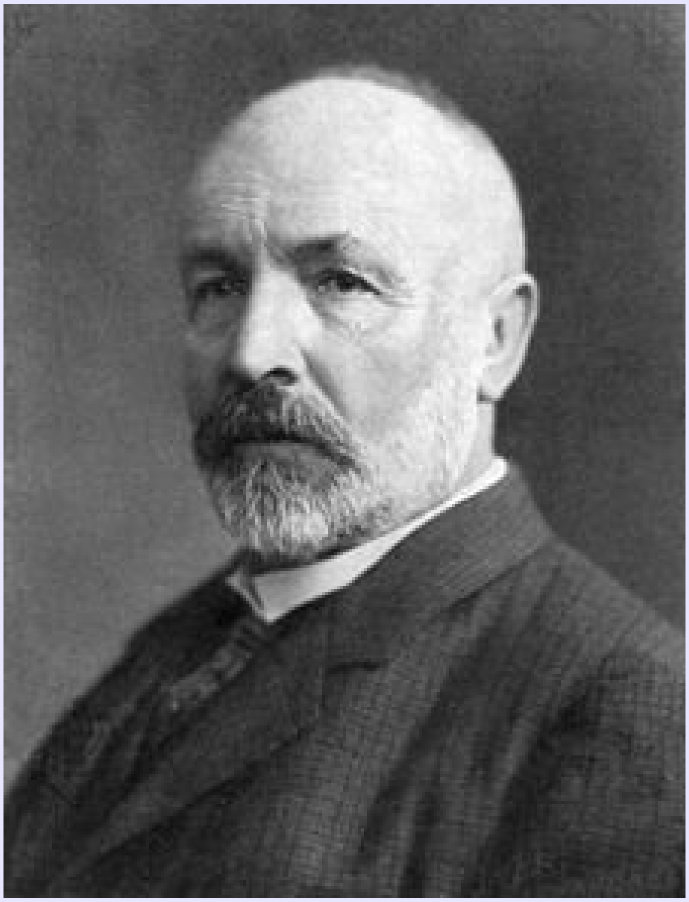
Not every magnitude that is a sum of infinitely many finite magnitudes is itself infinite.

§20 Ein merkwürdiges Verhältnis zweier unendlicher Mengen zueinander, bestehend darin, daß es möglich ist, jedes Ding der einen Menge mit dem der anderen so zu verbinden, daß kein einziges Ding in beiden Mengen ohne Verbindung bleibt, auch kein einziges in zwei oder mehr Paaren vorkommt.

A remarkable relationship between two infinite sets: it is possible to pair each object of the first set to one of the second such that every object in the two sets has a unique partner.

§21 Dennoch können beide unendliche Mengen, obschon mit Hinsicht auf die Vielheit ihrer Teile gleich, in einem Verhältnisse der Ungleichheit ihrer Vielheiten stehen, so daß die eine sich nur als ein Teil der anderen herausstellen kann.

And this situation can occur even if one of the sets is a proper subset of the other.



Georg Cantor (1845 – 1918)

- Cardinal numbers.

  Measuring the size of infinity and comparing the sizes of infinite sets.

- Ordinal numbers.

  Counting beyond infinity and providing the means of exhausting infinite sets by iterative processes.

- Cardinal numbers.

  Measuring the size of infinity and comparing the sizes of infinite sets.

- Ordinal numbers.

  Counting beyond infinity and providing the means of exhausting infinite sets by iterative processes.

- Cardinal numbers.

  Measuring the size of infinity and comparing the sizes of infinite sets.

Cantor, Georg (1874). Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen, *Journal für die reine und angewandte Mathematik*, 77, 258-262.

- Ordinal numbers.

  Counting beyond infinity and providing the means of exhausting infinite sets by iterative processes.

- Cardinal numbers.

  Measuring the size of infinity and comparing the sizes of infinite sets.

Cantor, Georg (1874). Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen, *Journal für die reine und angewandte Mathematik*, 77, 258-262.

- Ordinal numbers.

  Counting beyond infinity and providing the means of exhausting infinite sets by iterative processes.

Cantor, Georg (1872). Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen, *Mathematische Annalen*, 5, 123–132.

The dual nature of set theory.

- Historically, set theory started as a field of mathematics: the study of infinite sets and their relationships.
- In subsequent years, set theory developed into more than that: the standard foundations for mathematics.

Ernst Zermelo
1871–1953

Abraham Fraenkel
1891–1965

Thoralf Skolem
1887–1963

John von Neumann
1903–1957

In our course, we shall ignore the foundational side of set theory, and rather discuss basic set theory as a technique to deal with infinities.

A recurring theme of this course will be the fact that you can exhaust infinite sets by a procedure called transfinite recursion. As an application, this will be used in our final lecture (Friday) to produce an algorithm to determine the winner of an infinite game.

Basic set-theoretic techniques in logic
Part I: Measuring the infinite

Benedikt Löwe
Universiteit van Amsterdam
Grzegorz Plebanek
Uniwersytet Wrocławski

ESSLLI, Ljubljana August 2011

In the real world...

...sets have finitely many elements, e.g.

- $W = \{\mathrm{Mon}, \mathrm{Tue}, \ldots, \mathrm{Sat}\}$, $|W| = 7$;
- $EU = \{\mathrm{Austria}, \mathrm{Belgium}, \ldots, \mathrm{United\ Kingdom}\}$, $|EU| = 27$;
- $UN = \{\mathrm{Afghanistan}, \mathrm{Albania}, \ldots, \mathrm{Zimbabwe}\}$, $|UN| = 193$.

In mathematics ...

...many important sets are infinite, e.g.

- the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots, 2011, 2012, \ldots\}$;
- the set of rational numbers (all the quotients) $\mathbb{Q} = \{0, 1, 2, 2/3, 7/8, \ldots\}$;
- the set of all reals $\mathbb{R}$ (including $\mathbb{Q}$ and **many** other).

Although our world seems to be finite, we need the concept of infinity to describe it!
Saying that $\mathbb{N}$ and $\mathbb{R}$ are infinite, or writing $|\mathbb{N}| = |\mathbb{R}| = \infty$, is not enough.
In fact the symbol ∞ denotes rather *potential infinity*, e.g.

$$1 + 1/2 + 1/3 + \ldots = \infty,$$

while we shall discuss the *actual infinity*, of containing infinitely many elements. We shall see that infinity has many faces and we need several names for it.
It is intuitively clear that $\mathbb{N}$ is the 'smallest' infinite set.
It's infinite but countable, meaning: in theory, we can imagine naming all its elements.

Definition

We say that a set A is **countable** if we can write

$$A = \{a_1, a_2, \ldots, a_n, \ldots\}$$

where $a_1, a_2, \ldots$ are all distinct.

We can label all elements of a countable set A by natural numbers, so we think that A has the same number of elements as $\mathbb{N}$.

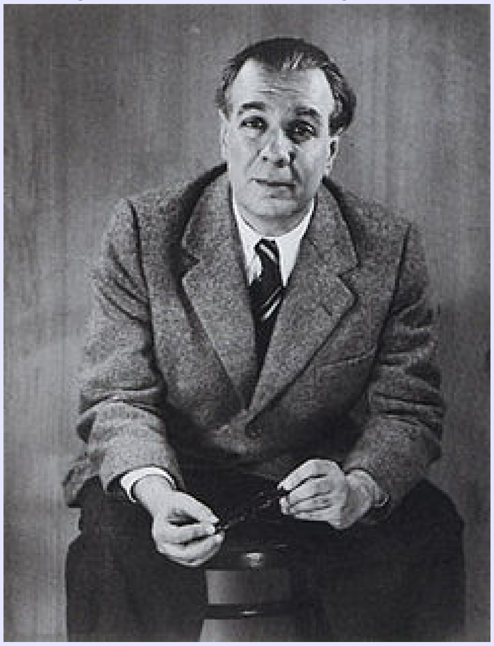
Aleph zero

The infinity represented by $\mathbb{N}$ is denoted by $\aleph_0$; we write

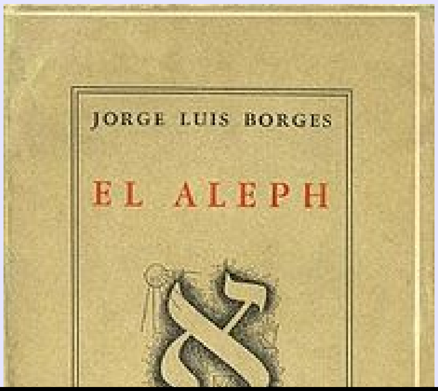
$$|\mathbb{N}| = \aleph_0.$$

Having introduced $\aleph_0$, we can write $|A| = \aleph_0$ instead of saying that A has as many elements as $\mathbb{N}$.

Why aleph? Why aleph with index 0? Why Borges?



Jorge Luis Borges (1899–1986)



Hotel $\aleph_0$

You are the owner of a hotel having inifnitely many rooms (numbered 1,2,...). Therefore if one day you have infinitely many guests $g_1, g_2, \ldots, g_n, \ldots$ then you can provide accomodation for all of them. Late in the evening another guest arrives? No problem:

$$g_1 \to 2, \quad g_2 \to 3, \quad \ldots, g_n \to n+1.$$

You will have the room no 1 free for the late guest.
Next day you face another infinite group of tourists $h_1, h_2, \ldots, h_n, \ldots$. Still no problem:

$$g_1 \to 2, \quad g_2 \to 4, \ldots, g_n \to 2n \ldots.$$

This makes all the rooms with odd numbers free, and

$$h_1 \to 1, \quad h_2 \to 3, \ldots, h_n \to 2n-1 \ldots.$$

Paradoxes of the infinite arise only when we attempt, with our finite minds, to discuss the infinite, assigning to it those properties which we give to the finite and limited. (Galileo)

Paradoxes? Rather theorems: $\aleph_0 + 1 = \aleph_0$, $\aleph_0 + \aleph_0 = \aleph_0$.

Properties of countable sets

- If A and B are countable then $A \cup B$ is countable.
- If A and B are countable then $A \times B$ is countable, too, where

$$A \times B = \{\langle a, b\rangle : a \in A, b \in B\}.$$

- If $A_1, A_2, \ldots$ are all countable then the set

$$A = A_1 \cup A_2 \cup \ldots A_n \cup \ldots$$

containing all elements of all those sets, is countable too.

Theorem

The set $\mathbb{Q}$ of rational numbers is countable: $|\mathbb{Q}| = \aleph_0$.

Theorem

The set $\mathbb{R}$ of all real numbers is not countable.

Proof.

In fact we shall check that already the interval $[0, 1]$ is not countable.
Suppose that we have managed to create a list $a_1, a_2, \ldots$ of all real numbers $x \in [0, 1]$.

number	0.	1st	2nd	3rd	...	nth	...
a_1	0.	? x_1					
a_2	0.		? x_2				
a_3	0.			? x_3			
...	0.						
a_n	0.					? x_n	
...	0.						

The number $0.x_1x_2 \ldots x_n \ldots$ is not on our list!

Definition

The cardinality of $\mathbb{R}$ is called **continuum** and denoted by $\mathfrak{c}$:

$$|\mathbb{R}| = \mathfrak{c}.$$

Why not $\aleph_1$? Be patient!

Comparing arbitrary sets

- We say that two sets X and Y are **equinumerous** if there is a bijection $f : X \to Y$, that is one-to-one correspondence between all elements of X and all elements of Y.
- Equinumerous sets have the same cardinality: $|X| = |Y|$.
- Note that a set X is countable if it is equinumerous with $\mathbb{N}$.

Examples

- Every two nonempty intervals (a, b) and (c, d) on the real line are equinumerous and have cardinality $\mathfrak{c}$.
- **Theorem.** The plane $\mathbb{R} \times \mathbb{R}$ is equinumerous with $\mathbb{R}$.
- All the Euclidean spaces $\mathbb{R}^1, \mathbb{R}^2, \ldots, \mathbb{R}^d, \ldots$ have cardinality $\mathfrak{c}$.

Comparing arbitrary sets II

- $|X| \leq |Y|$ if there is a one-to-one function $f : X \to Y$, that is a bijection between X and some part of Y.
- $|X| < |Y|$ if $|X| \leq |Y|$ but $|X| \neq |Y|$.

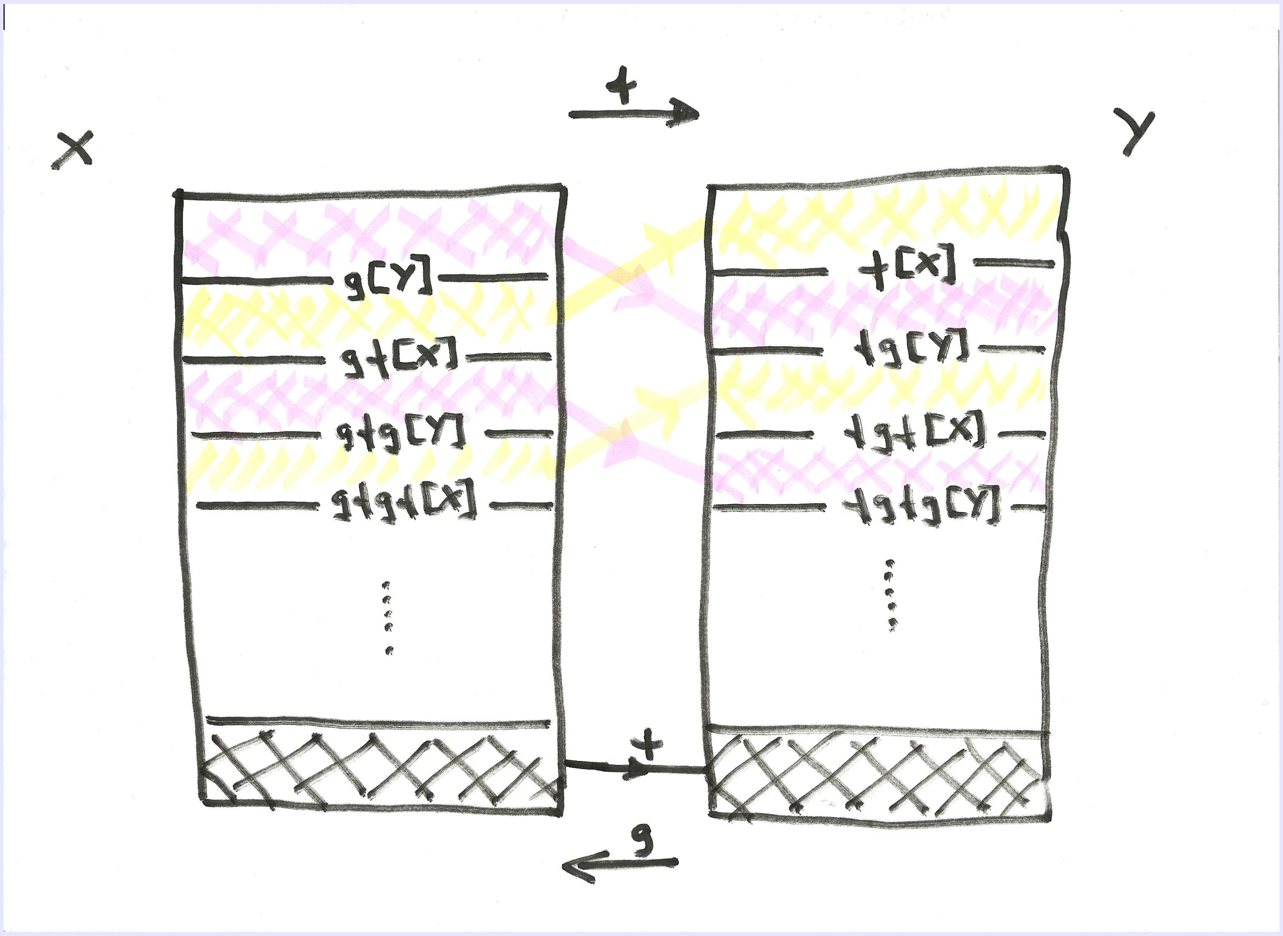
We already know that $|\mathbb{N}| < |\mathbb{R}|$, in other words: $\aleph_0 < \mathfrak{c}$.

Theorem (Cantor-Bernstein)

If $|X| \leq |Y|$ and $|Y| \leq |X|$ then $|X| = |Y|$.

Do not think it's obvious!

A math lecture without a proof is like a movie without a love scene. (H. Lenstra)



Definition

If X is any set we denote by $P(X)$ the power set of X, that is the family of all subsets of X.

Example

Let $X = \{1, 2, 3\}$. Then

$$P(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

If $X = \{1, 2, \ldots, n\}$ then $P(X)$ has 2^n elements.

Definition

If X is a set of cardinality κ then 2^κ denotes the cardinality of $P(X)$.

For a finite set X we have $2^{|X|} > |X|$ since $2^n > n$.

Theorem (Cantor)

For every set X the power set $P(X)$ has more elements than X; in other words

$$2^{\kappa} > \kappa,$$

for any cardinal number.

Proof.

We have $|X| \leq |P(X)|$ since we can define one-to-one function $f : X \to P(X)$ by $f(x) = \{x\}$.
Suppose that $g : X \to P(X)$ is a bijection. Consider the set $A \subseteq X$, where

$$A = \{x \in X : x \notin g(x)\}.$$

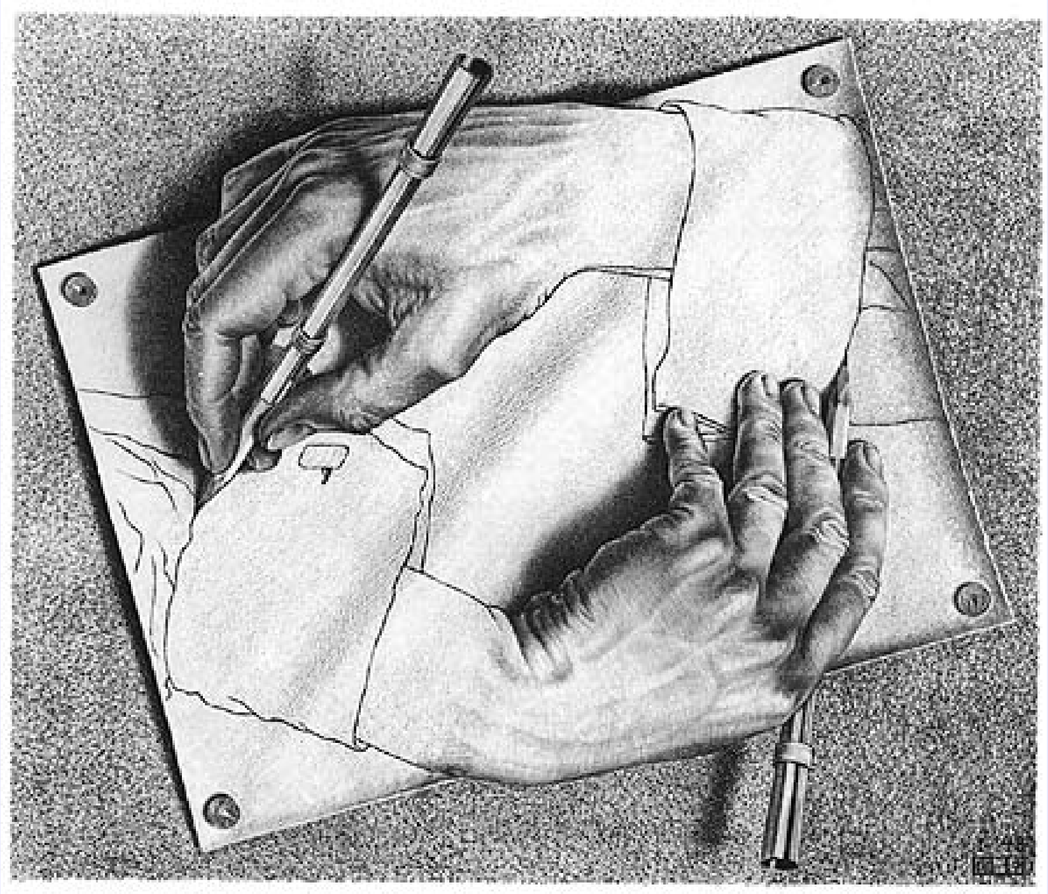
Then A cannot be associated with any $x \in X$. If we suppose that $A = g(x_0)$ then we have a puzzle whether x_0 is in A or not:

- if $x_0 \in A$ then $x_0 \notin g(x_0) = A$;
- if $x_0 \notin A$ then $x_0 \in g(x_0) = A$,

a contradiction!. $\square$

Like in a famous **Barber paradox:**

In some village there was one man who was the only barber and he was ordered to shave all the men who do not shave themselves. Should he shave himself?



‘Drawing hands’ by Maurits Cornelis Escher

Conclusions

- $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \ldots$;
- there are **infinitely** many kinds of infinity;
- there is no set X which is the biggest one.

What about $\mathfrak{c}$? We shall see that

Theorem

$$\mathfrak{c} = 2^{\aleph_0}$$

We can also ask if there are only **countably** many types of infinity:-)

An application: Transcendental numbers

- Recall that $x \in \mathbb{R}$ is rational if $x = a/b$ for some integers a, b, $b \neq 0$.
- $\sqrt{2}$ is not rational but it solves the equation $x^2 - 2 = 0$.
- x is **algebraic** if x is a solution of some equation

$$a_0 + a_1x + a_2x^2 + \ldots a_nx^n = 0,$$

  for some integers a_i and some n.
- π and $e = \lim_{n\to\infty}(1 + 1/n)^n$ are not algebraic, they are **transcendental**. But it's difficult to prove it!
- Is there is an easy way of showing that there are transcendental numbers?
- The set of all algebraic numbers is countable; so a *typical number* is indeed transcendental.

Basic set-theoretic techniques in logic
Part II, Counting beyond infinity: Ordinal numbers

Benedikt Löwe
Universiteit van Amsterdam
Grzegorz Plebanek
Uniwersytet Wrocławski

ESSLLI, Ljubliana August 2011

Summary of the first lecture:
We have discussed how to measure the infinity, in particular measuring the size of the set o natural numbers:

$$\aleph_0$$

Now for something slightly different. Have you ever counted up to 1000?

$$1, 2, 3, \ldots, 1000.$$

It takes more than 16 minutes but surely we can do it.
We can also imagine ourselves counting up to $10^{10^{10}}$ though it will be really time-consuming.
Can we count beyond infinity? If so we need a new name:

Having ω (sometimes denoted ω_0) at hand we can continue:

$$0, 1, 2, \ldots, 2011, \ldots, \omega, \omega+1, \omega+2, \ldots, \omega+\omega, \ldots$$

Is there any use of this?

Pros and Cons of Hitch Hiking[a]

[a] after Roger Waters, ex Pink Floyd

- Suppose you are hitchhiking from A to B.
- Pros: should be for free.
- Cons: the route may be complicated,
- starting from $A \to B$ (0 stops), to
- $A \to S_1 \to B$ (1 stop),
- $A \to S_1 \to S_2 \to B$ (2 stops),
- and so on.

Pros and Cons of Hitch Hiking, continued

Suppose that on our way we may be offered a lift by little dwarfs in their little cars, moving us only a tiny little bit forward:

$$A \to S_1 \to S_2 \to \ldots \to S_n \to \ldots \to B.$$

Then we may call such a route ω. Can you imagine hitchhiking in the $\omega + 1$ or $\omega + \omega$ style?

All the hitchhiker's routes

Denote the collection of all possible routes by ω_1;

$$\omega_1 = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2 \ldots, \omega + \omega, \omega + \omega + 1, \ldots\}.$$

- Note that $1 + \omega$ is the same as ω but $\omega + 1$ is different.
- With every route α we can think of $\alpha + 1$, so there is no largest element of ω_1.
- Every route α has finitely or countably many stops.
- If α is a route and X is any nonempty set of stops appearing in α then X has the first stop.
- If $\alpha_1, \alpha_2, \ldots$ is any sequence of routes then there is a route α which is more complicated than all α_n's.
- The set ω_1 of all routes is uncountable.

Now a serious stuff!

Definition

We say that a set X is **linearly ordered** by $<$ if for any $x, y, z \in X$

- $x \not< x$;
- $x < y$ and $y < z$ imply $x < z$;
- if $x \neq y$ then $x < y$ or $y < x$.

Example

The set $\mathbb{R}$ of reals is linearly ordered by the 'natural' order.
All words are linearly ordered by the lexicographic order.

Definition

A set X is **well-ordered** by $<$ if it is linearly ordered and

- every nonempty subset A of X has a least element.

Example

The set $\mathbb{N}$ is well-ordered. Hmmmm, should be obvious...
The interval $[0, 1]$ has the least element $(= 0)$ but is not well-ordered because its subset $A = \{1, 1/2, 1/3, \ldots\}$ does not contain a least element.

Definition

Two well-ordered sets $(X, <)$ and $(Y, <)$ are **isomorphic** if there is a bijection $f : X \to Y$ such that

- $x_1 < x_2$ is equivalent to $f(x_1) < f(x_2)$;

for any $x_1, x_2 \in X$.

Theorem

1. *If $(X, <)$ is well-ordered and $f : X \to X$ is an increasing function then $f(x) \geq x$ for every $x \in X$.*
2. *If $(X, <)$ is well-ordered and $f : X \to X$ is an isomorphism then f is the identity function.*

Proof.

Suppose that $f(x) \geq x$ does not hold for all x; it means that the set

$$A = \{x \in X : f(x) < x\}$$

is nonempty. Take its minimal element x_0. Then $y_0 = f(x_0) < x_0$ (since $x_0 \in A$), and $f(y_0) < f(x_0) = y_0$ (since f is increasing). It follows that $y_0 \in A$, a contradiction with $y_0 < x_0$.
By the first part we have $f(x) \geq x$ for any x. We can also apply the first part to the inverse function $f^{-1} : X \to X$:
$f^{-1}(x) \geq x$ so $x = f(f^{-1}(x)) \geq f(x)$.
Hence $f(x) = x$ for all x.

□

If X is well-ordered and $a \in X$ then the set $\{x \in X : x < a\}$ is called **the initial segment** of X given by a.

Theorem

Let $(X, <)$ and $(Y, <)$ be two well-ordered sets. Then either

1. *X and Y are isomorphic, or*
2. *X is isomorphic to some initial segment of Y, or*
3. *Y is isomorphic to some initial segment of X.*

Definition

An **ordinal number** is the order type of some well-ordered set.

If α is the order type of X and β is the order type of Y then

1. $\alpha = \beta$,
2. $\alpha < \beta$,
3. $\beta < \alpha$,

in the corresponding cases.

Example

- 0 is the order type of the empty set;
- 1 is the order type of a set consisting of one element;
- $\omega = \omega_0$ is the order type of $\{0, 1, 2, \ldots\}$;

We may as well think that ω **is** the set $\{0, 1, 2, \ldots\}$.

Definition

ω_1 is the least order type of a well-ordered uncountable set.

We have $\alpha < \omega_1$ whenever α is an order type of a countable set. We may think that $\omega_1 = \{0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \alpha, \ldots\}$ is the set of all order types of countable sets.

Ordinal and cardinal numbers

- An ordinal number α is a cardinal number if for every $\beta < \alpha$ we have $|\beta| < |\alpha|$.
- $0, 1, 2, \ldots$ are cardinal numbers.
- ω is a cardinal number (denoted $\aleph_0$).
- $\omega + 1$, $\omega + \omega$ are not cardinal numbers.
- ω_1 is the next cardinal number denoted as $\aleph_1$.
- ω_2 is the least order type of a set of cardinality $> \aleph_1$; $\aleph_2 = \omega_2$.
- We can define $\aleph_0 < \aleph_1 < \aleph_2 < \ldots$.
- Then $\aleph_\omega$ comes. **And so on . . .** Do you understand?[a]

[a] In mathematics, you don't understand things. You just get used to them. (John von Neumann)

Handling the continuum

- We have an exact list of cardinal numbers $\aleph_0 < \aleph_1 < \aleph_2 < \ldots$.
- Before we defined another list $\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \ldots$.
- We also considered $\mathfrak{c}$ — the cardinality of $\mathbb{R}$.
- Let us prove that $\mathfrak{c} = 2^{\aleph_0}$.

$2^{\aleph_0} = \mathfrak{c}$.

Note that $2^{\aleph_0}$ (by the definition the cardinality of $P(\mathbb{N})$) is the cardinality of the set $\{0,1\}^{\mathbb{N}}$ of all infinite sequences of of 0's and 1's.

The function $f : \{0,1\}^{\mathbb{N}} \to \mathbb{R}$, where

$$f(x_1, x_2, \ldots) = \sum_{n=1}^{\infty} \frac{2x_n}{3^n},$$

is one-to-one. It follows that $2^{\aleph_0} \leq \mathfrak{c}$.

Every $x \in [0,1]$ has a unique **infinite** binary expansion

$$x = (0, x_1 x_2 \ldots)_{(2)}.$$

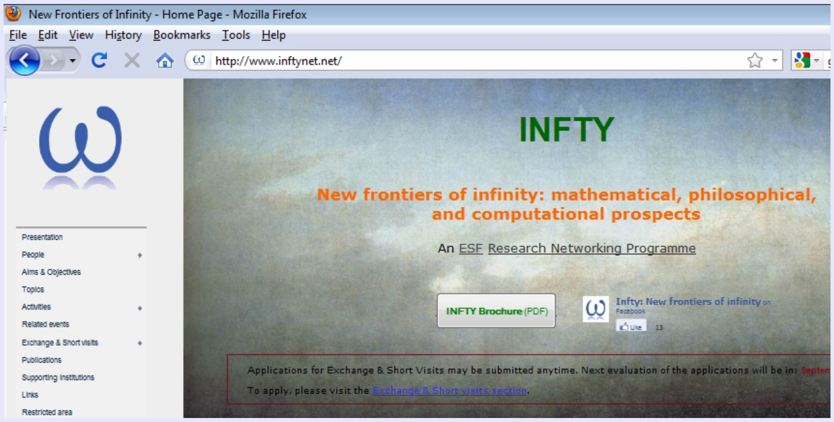
This shows that $[0,1]$ admits one-to-one function into $\{0,1\}^{\mathbb{N}}$, and $\mathfrak{c} = |[0,1]| \leq 2^{\aleph_0}$. Finally $\mathfrak{c} = 2^{\aleph_0}$ by the Cantor-Bernstein theorem. $\square$

Basic set-theoretic techniques in logic
Part III, Transfinite recursion and induction

Benedikt Löwe
Universiteit van Amsterdam
Grzegorz Plebanek
Uniwersytet Wrocławski

ESSLLI 2011, Ljubljana, Slovenia

Both the workshop *Modern Set Theory: Foundations & Applications* and the foundational course *Ordinals and Cardinals: Basic set-theoretic techniques in logic* are generously funded by the European Science Foundation in the research networking programme INFTY.



http://www.math.uni-hamburg.de/home/loewe/INFTY@ESSLLI2011/

Today...

$$\aleph_0 < \aleph_1 < \aleph_2 < \dots$$

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$$

1. Mirna's question: how do you construct an uncountable ordinal?
2. The Continuum Hypothesis
3. Induction and Recursion on $\mathbb{N}$
4. Transfinite Induction and Recursion
5. A few applications

Reminder (1).

Two equivalence relations:

- $|X| = |Y|$: X and Y are equinumerous; i.e., there is a bijection between X and Y.
- $(X, R) \simeq (Y, S)$: (X, R) and (Y, S) are isomorphic as ordered structures; i.e., there is an order-preserving bijection between X and Y.

The cardinalities are the equivalence classes of the equivalence relation of being equinumerous; the ordinals are the equivalence classes of being order-isomorphic.

Note that if $(X, R) \simeq (Y, S)$, then $|X| = |Y|$. The converse doesn't hold: $|\omega + 1| = |\omega|$, but $\omega + 1 \not\simeq \omega$. We called an ordinal κ a cardinal if for all $\alpha < \kappa$, we have $|\alpha| < |\kappa|$.

Reminder (2).

A structure (X, R) was called a wellorder if (X, R) is a linear order and every nonempty subset of X has an R-least element.

Proposition. The following are equivalent for a linear order (X, R):

1. (X, R) is a well-order, and
2. there is no infinite R-descending sequence, i.e., a sequence $\{x_i; i \in \mathbb{N}\}$ such that for every i, we have $x_{i+1} R x_i$.

Proof. "1⇒2". If $X_0 := \{x_i; i \in \mathbb{N}\}$ is an R-descending sequence, then X_0 is a nonempty subset of X without R-least element.

"2⇒1". Let $Z \subseteq X$ be a nonempty subset without R-least element. Since it is nonempty, there is a $z_0 \in Z$. Since it has no R-least element, for each $z \in Z$, the set $B_z := \{x \in Z; xRz\}$ is nonempty.

For each z, pick an element $b(z) \in B_z$. Now define by recursion $z_{n+1} := b(z_n)$. The defined sequence $\{z_n; n \in \mathbb{N}\}$ is R-descending by construction. q.e.d.

Mirna's question: how do you construct an uncountable ordinal?

Hartogs' Theorem. If X is a set, then we can construct a well-order (Y, R) such that $|Y| \not\leq |X|$.

We'll prove the special case of $X = \mathbb{N}$ and thus prove that there is an uncountable ordinal:

Consider

$$H := \{(X, R) \; ; \; X \subseteq \mathbb{N} \text{ and } (X, R) \text{ is a wellorder}\}.$$

We can order H by

$(X, R) \prec (Y, S)$
iff (X, R) is isomorphic to a proper initial segment of (Y, S).

How do you construct an uncountable ordinal? (2)

$$H := \{(X, R)\ ;\ X \subseteq \mathbb{N} \text{ and } (X, R) \text{ is a wellorder}\}.$$

$$(X, R) \prec (Y, R) \text{ iff } (X, R) \text{ is isomorphic to a proper initial segment of } (Y, S).$$

1. $(H, \prec)$ is a linear order.
2. $(H, \prec)$ is a wellorder.
3. H is closed under initial segments: if $(X, R) \in H$ and $(Y, R{\restriction}Y)$ is an initial segment of (X, R), then $(Y, R{\restriction}Y) \in H$. So in particular, if α is the order type of some element of H, then the order type of $(H, \prec)$ must be at least α.
4. If α is the order type of some element of H, then $\alpha + 1$ is.

Claim. H cannot be countable.

In fact, we have *constructed* a wellorder of order type ω_1.

The continuum hypothesis

- $\aleph_1$ is the least cardinal greater than $\aleph_0$.
- $\mathfrak{c}$ is the cardinality of the real line $\mathbb{R}$.
- It is not obvious at all that there is **any** relation between $\aleph_1$ and $\mathfrak{c}$, as we do not know whether there is a cardinal that is equinumerous to $\mathbb{R}$ (see the Thursday lecture).
- If we assume that $\mathfrak{c}$ is a **cardinal** and not just a cardinality, then we know that $\mathfrak{c} \geq \aleph_1$ since cardinals are linearly ordered.
- Cantor conjectured (in 1877) that in fact $\mathfrak{c} = \aleph_1$. This statement is called **the Continuum Hypothesis** (CH).
- CH was the first problem on the famous Hilbert list (1900).
- In 1938, Kurt Gödel proved that there is a model of set theory in which CH holds.
- In 1963, Paul Cohen proved that you cannot prove CH. In fact, for any $n \geq 1$, the statement $\mathfrak{c} = \aleph_n$ is consistent. With a few exceptions (e.g., $\aleph_\omega$), $\mathfrak{c}$ can be any $\aleph_\alpha$.

Induction on the natural numbers (1).

The induction principle (IP).

Suppose $X \subseteq \mathbb{N}$. If

- $0 \in X$, and
- $n \in X$ implies $n+1 \in X$,

then $X = \mathbb{N}$.

Example. The proof of "There are countably many polynomials with integer coefficients":

$$P = P_1 \cup P_2 \cup P_3 \cup \ldots$$

If we can show that each P_i is countable, then P is countable as a countable union of countable sets.

Define

$$X := \{n \; ; \; P_{n+1} \text{ is countable}\}$$

Induction on the natural numbers (2).

$$X := \{n \; ; \; P_{n+1} \text{ is countable}\}$$

$0 \in X$. An element of P_1 is of the form $ax + b$ for $a, b \in \mathbb{Z}$, so $|P_1| = \mathbb{Z} \times \mathbb{Z}$. Thus P_1 is countable, and $0 \in X$.

if $n \in X$, then $n + 1 \in X$. Suppose $n \in X$, that means that P_{n+1} is countable. Take an element of P_{n+2}. That is of the form

$$a_{n+2}x^{n+2} + a_{n+1}x^{n+1} + a_n x^n + ... + a_0 = a_{n+2}x^{n+2} + p$$

for some $p \in P_{n+1}$. So, $|P_{n+2}| = |\mathbb{Z} \times P_{n+1}|$, and thus (because P_{n+1} was countable), P_{n+2} is countable.

The induction principle now implies that $X = \mathbb{N}$, and this means that P_n is countable for all n.

The least number principle.

The least number principle (LNP).

Every nonempty subset of $\mathbb{N}$ has a least element.

This means: $(\mathbb{N}, <)$ is a wellorder.

(Meta-)Theorem. If LNP holds, then IP holds.

Proof. Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \mathbb{N}$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n+1 \in X$.

Consider $Y := \mathbb{N} \backslash X$. Since $X \neq \mathbb{N}$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n + 1$ for some $n \in \mathbb{N}$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n + 1 \in X$, but that's a contradiction to our assumption. q.e.d.

Recursion on the natural numbers (1).

The recursion principle (RP).

Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a function and $n_0 \in \mathbb{N}$. Then there is a unique function $F : \mathbb{N} \to \mathbb{N}$ such that

- $F(0) = n_0$, and
- $F(n+1) = f(F(n))$ for any $n \in \mathbb{N}$.

Two ways to define addition and multiplication on the natural numbers:

1. "cardinal-theoretic": $n + m$ is the unique natural number k such that any set that is the disjoint union of a set of n elements with a set of m elements has k elements.
2. "recursive": Fix n. Define a function addto_n by recursion ("Grassmann equalities"):

$$\mathrm{addto}_n(0) := n, \text{ and}$$
$$\mathrm{addto}_n(m+1) := \mathrm{addto}_n(m) + 1.$$

Define $n + m := \mathrm{addto}_n(m)$.

Recursion on the natural numbers (1).

The recursion principle (RP).

Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a function and $n_0 \in \mathbb{N}$. Then there is a unique function $F : \mathbb{N} \to \mathbb{N}$ such that

- $F(0) = n_0$, and
- $F(n+1) = f(F(n))$ for any $n \in \mathbb{N}$.

Is RP obvious?

No, since the recursion equations are not an allowed form of definition: in the definition of the objection F, you are referring to F itself.

Proof. We'll prove RP from IP.

What do we have to prove? We need to give a concrete definition of F, i.e., a formula $\varphi(n, m)$ that holds if and only if $F(n) = m$.

Recursion on the natural numbers (2).

Preliminary work:

If $g : \{0, ..., m\} \to \mathbb{N}$ is a function such that

- $g(0) = n_0$, and
- $g(n+1) = f(g(n))$ for any $n < m$,

we call it a germ of length m.

1. The function $g_0 : \{0\} \to \mathbb{N}$ defined by $g_0(0) := n_0$ is a germ of length 0.
2. If g is a germ of length m and $k < m$, then $g \restriction \{0, ..., k\}$ is a germ of length k.
3. If g is a germ of length m, then the function g^* defined by

$$g^*(k) := \begin{cases} g(k) & \text{if } k \leq m, \\ f(g(m)) & \text{if } k = m+1. \end{cases}$$

   is a germ of length $m+1$.
4. For every $n \in \mathbb{N}$, there is a germ of length n.
5. If g, h are germs of length n, then $g = h$.

Recursion on the natural numbers (3).

(RP) Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a function and $n_0 \in \mathbb{N}$. Then there is a unique function $F : \mathbb{N} \to \mathbb{N}$ such that

- $F(0) = n_0$, and
- $F(n+1) = f(F(n))$ for any $n \in \mathbb{N}$.

What do we have to prove? We need to give a concrete definition of F, i.e., a formula $\varphi(n, m)$ that holds if and only if $F(n) = m$.

We have proved that for every $n \in \mathbb{N}$, there is a unique germ of length n, let's call it g_n. Here is our definition of F:

$$\varphi(n, m) \iff m = f(g_n(n)).$$

Counting beyond infinity.

We have defined the ordinals (essentially) as wellorders, i.e., sets that satisfy what we called the least number principle. For $\mathbb{N}$, we showed that LNP implies IP, so maybe we can prove a transfinite induction principle?

First attempt at a transfinite induction principle.

Suppose α is an ordinal and $X \subseteq \alpha$. If

- $0 \in X$, and
- $\beta \in X$ implies $\beta + 1 \in X$,

then $X = \alpha$.

Can this be true? Let $\alpha = \omega + 1 = \{0, 1, 2, 3, ..., 2011, ..., \omega\}$ and consider $X = \{0, 1, 2, 3, ..., 2011, ...\}$. Then X satisfies the two conditions in the induction principle, but $X \neq \omega + 1$.

So, our first attempt didn't work.

That's strange...

We proved that LNP implies IP (for $\mathbb{N}$) and all ordinals satisfy LNP, so why don't they also satisfy IP?

We need to analyse what goes wrong in our proof in the case of $\omega + 1$ and X:

Proof of "LNP implies IP".

Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \mathbb{N}$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n + 1 \in X$.

Consider $Y := \mathbb{N} \backslash X$. Since $X \neq \mathbb{N}$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n + 1$ for some $n \in \mathbb{N}$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n + 1 \in X$, but that's a contradiction to our assumption. q.e.d.

That's strange...

We proved that LNP implies IP (for $\mathbb{N}$) and all ordinals satisfy LNP, so why don't they also satisfy IP?

We need to analyse what goes wrong in our proof in the case of $\omega + 1$ and X:

Proof of "LNP implies IP".

Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \omega + 1$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n + 1 \in X$.

Consider $Y := \omega + 1 \backslash X$. Since $X \neq \omega + 1$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n + 1$ for some $n \in \omega + 1$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n + 1 \in X$, but that's a contradiction to our assumption. q.e.d.

That's strange...

We proved that LNP implies IP (for $\mathbb{N}$) and all ordinals satisfy LNP, so why don't they also satisfy IP?

We need to analyse what goes wrong in our proof in the case of $\omega + 1$ and X:

Proof of "LNP implies IP".

Suppose that LNP holds, but IP doesn't. So, there is some $X \neq \omega + 1$ satisfying the conditions of IP, i.e., $0 \in X$ and "if $n \in X$, then $n + 1 \in X$.

Consider $Y := \omega + 1 \backslash X$. Since $X \neq \omega + 1$, this is a nonempty set. By LNP, it has a least element, let's call it y_0.

Because $0 \in X$, it cannot be that $y_0 = 0$. Therefore, it must be the case that $y_0 = n + 1$ for some $n \in \omega + 1$. In particular, $n < y_0$. But y_0 was the least element of Y, and thus $n \notin Y$, so $n \in X$.

Now we apply the induction hypothesis, and get that $y_0 = n + 1 \in X$, but that's a contradiction to our assumption. q.e.d.

Successor ordinals and limit ordinals.

We say that an ordinal α is a successor ordinal if there is some β such that $\alpha = \beta + 1$. If that is not the case, then α is called a limit ordinal.

Examples.

$$1 = 0 + 1$$
$$17 = 16 + 1$$
$$2001 = 2010 + 1$$
$$\omega + 17 = (\omega + 16) + 1$$

But ω, $\omega + \omega$, $\omega + \omega + \omega$, and also ω_1, ω_2 etc. do not have this property, and thus are limit ordinals.

Transfinite induction (1).

Transfinite induction principle.

Suppose α is an ordinal and $X \subseteq \alpha$. If

- $0 \in X$,
- $\beta \in X$ implies $\beta + 1 \in X$, and
- if $\lambda < \alpha$ is a limit ordinal and for all $\beta < \lambda$, we have $\beta \in X$, then $\lambda \in X$,

then $X = \alpha$.

Transfinite induction (2).

Proof of TIP. Suppose α is an ordinal, i.e., wellordered, but TIP doesn't hold. So, there is some $X \neq \alpha$ satisfying the conditions of TIP, i.e.,

- $0 \in X$,
- $\beta \in X$ implies $\beta + 1 \in X$, and
- if $\lambda < \alpha$ is a limit ordinal and for all $\beta < \lambda$, we have $\beta \in X$, then $\lambda \in X$.

Consider $Y := \alpha \backslash X$. Since $X \neq \alpha$, this is a nonempty set. By the fact that α is wellordered, it has a least element, let's call it y_0.

The element y_0 has to be either a successor or a limit ordinal. If it is a successor, then $y_0 = \beta + 1$ for some $\beta \in X$, but then $y_0 \in X$. If it is a limit, then all of its predecessors are in X, and thus $y_0 \in X$. This gives the desired contradiction. q.e.d.

Transfinite recursion.

Suppose that α is an ordinal. We call a function $s : \beta \to \mathrm{Ord}$ a segment if $\beta < \alpha$. Suppose that you have an ordinal α_0, a function $f : \mathrm{Ord} \to \mathrm{Ord}$ and a function g assigning an ordinal to every segment.

Then there is a unique function $F : \alpha \to \mathrm{Ord}$ such that

1. $F(0) = \alpha_0$,
2. $F(\beta + 1) = f(F(\beta))$, if $\beta + 1 \in \alpha$, and
3. $F(\lambda) = g(F \restriction \lambda)$ if $\lambda \in \alpha$ is a limit ordinal.

The proof is a homework exercise.

Global version of transfinite recursion.

Suppose that you have an ordinal α_0, a function $f : \mathrm{Ord} \to \mathrm{Ord}$ and a function g assigning an ordinal to every segment.

Then there is a unique set operation $F : \mathrm{Ord} \to \mathrm{Ord}$ such that

1. $F(0) = \alpha_0$,
2. $F(\beta + 1) = f(F(\beta))$, for every β, and
3. $F(\lambda) = g(F{\restriction}\lambda)$ if λ is a limit ordinal.

First application:

$$\begin{aligned} \aleph_0 &:= \omega, \\ \aleph_{\beta+1} &:= \text{the least ordinal } \gamma \text{ such that } |\aleph_\beta| < |\gamma|, \\ \aleph_\lambda &:= \text{the least ordinal } \gamma \text{ such that } |\aleph_\beta| < |\gamma| \text{ for all } \beta < \lambda. \end{aligned}$$

$$\begin{aligned} \beth_0 &:= \omega, \\ \beth_{\beta+1} &:= |2^{\beth_\beta}| \\ \beth_\lambda &:= \text{the least ordinal } \gamma \text{ such that } |\beth_\beta| < |\gamma| \text{ for all } \beta < \lambda. \end{aligned}$$

Ordinal arithmetic (1).

Two ways to define ordinal addition:

1. "order-theoretic": $\alpha + \beta$ is the unique ordinal corresponding to the wellorder of the disjoint union of α and β where all elements of α precede all elements of β.
2. "recursive": Fix α. Define a function addto_α by recursion:

$$\begin{aligned}
\mathrm{addto}_\alpha(0) &:= \alpha, \\
\mathrm{addto}_\alpha(\beta+1) &:= \mathrm{addto}_\alpha(\beta) + 1, \\
\mathrm{addto}_\alpha(\lambda) &:= \text{the least } \gamma \text{ bigger than all } \mathrm{addto}_\alpha(\beta) \text{ for } \beta < \lambda.
\end{aligned}$$

Define $\alpha + \beta := \mathrm{addto}_\alpha(\beta)$.

And based on this, ordinal multiplication:

$$\begin{aligned}
\mathrm{mult}_\alpha(0) &:= 0, \\
\mathrm{mult}_\alpha(\beta+1) &:= \mathrm{mult}_\alpha(\beta) + \alpha, \\
\mathrm{mult}_\alpha(\lambda) &:= \text{the least } \gamma \text{ bigger than all } \mathrm{mult}_\alpha(\beta) \text{ for } \beta < \lambda.
\end{aligned}$$

$\alpha \cdot \beta := \mathrm{mult}_\alpha(\beta)$.

Basic set-theoretic techniques in logic
Part IV: The Axiom of Choice

Benedikt Löwe
Universiteit van Amsterdam
Grzegorz Plebanek
Uniwersytet Wrocławski

ESSLLI, Ljubljana August 2011

Why axioms?

If we start playing with sets without any care we are in trouble:

The Russell paradox

Suppose that there is a set X such that

$$X = \{a : a \notin a\}.$$

Then $X \in X \iff X \notin X$, which is a false sentence.

Therefore we start by a list of axioms naming some legitimate operations.

The Russell paradox show that it is not always possible to form a set of the form $\{x : \varphi(x)\}$.

Some axioms of Zermelo-Fraenkel (ZF)

- **Union:** For any sets X and Y there is a set, denoted $X \cup Y$, containing all elements of X and all elements of Y.
- **Separation:** If A is a set and φ is some property then there is a set $\{x \in A : \varphi(x)\}$.
- **Power set:** For every set X there is a set $\{A : A \subseteq X\}$ (denoted $P(X)$).
- **Infinity:** There is an infinite set.

The axiom of choice (AC)

For every family $\mathcal{A}$ of nonempty sets there is a choice function f, such that $f(A) \in A$ for every $A \in \mathcal{A}$.

ZF+ AC=ZFC.

Equivalent forms

1. **The axiom of choice.**
2. **Zermelo's theorem:** Every set can be well-ordered.

Proof.

(1)⟶(2) Take any set X. We shall show that $X = \{x_\alpha : \alpha < \gamma\}$ for some ordinal number γ.
Let f be a choice function for the family of all nonempty subsets of X. We define

$$x_\alpha = f(X \setminus \{x_\beta : \beta < \alpha\}),$$

until it is possible. Then take γ to be the first ordinal number for which the set $X \setminus \{x_\alpha : \alpha < \gamma\}$ is empty.
(2)⟶(1) If $\mathcal{A}$ is any family of nonempty sets then we can order the union $X = \bigcup \mathcal{A}$ of all of them and define $f(A)$ to be the first element of A. □

Zorn's lemma, Tuckey style

Theorem

Let X be a set and $\mathcal{A}$ be a family of its subsets. Assume that $\mathcal{A}$ has finite character, i.e. $B \in \mathcal{A}$ if and only if all finite subsets of B belong to $\mathcal{A}$.
Then for any $A \in \mathcal{A}$ there is $M \in \mathcal{A}$ such that $A \subseteq M$ and M is maximal, i.e. for every $M' \in \mathcal{A}$ satisfying $M \subseteq M'$ we have $M' = M$.

Proof.

Let $X = \{x_\alpha : \alpha < \gamma\}$. Define M by

$$x_\alpha \in M \Leftrightarrow A \cup \{x_\beta \in M : \beta < \alpha\} \cup \{x_\alpha\} \in \mathcal{A}.$$

Then $M \in \mathcal{A}$ because all the finite subsets of M are in $\mathcal{A}$. $\square$

Application: Hamel basis

A set $\{x_1, x_2, \ldots, x_n\}$ of reals is linearly independent over $\mathbb{Q}$ if for any $q_i \in \mathbb{Q}$, if $q_1x_1 + q_2x_2 + \ldots + q_nx_n = 0$ then $q_i = 0$ for all $i \leq n$.

Example

$\{1, \sqrt{2}, \sqrt{3}\}$ is linearly independent over $\mathbb{Q}$.

Remark

If $\{x_1, x_2, \ldots, x_n\}$ is l.i. while $\{x_1, x_2, \ldots, x_n, y\}$ is not then $y = q_1x_1 + \ldots q_nx_n$ for some q_i's.

Theorem

There is a maximal linearly independent over $\mathbb{Q}$ set $H \subseteq \mathbb{R}$. Every $x \in \mathbb{R}$ has the unique representation $x = \sum_{i \leq n} q_i h_i$, where $n \in \mathbb{N}$, $q_i \in \mathbb{Q}$, $h_i \in H$.

Application: Vitali sets

For $x, y \in \mathbb{R}$, say that $x \sim y$ if $x - y \in \mathbb{Q}$. The relation is equivalence relation on $\mathbb{R}$, that is $x \sim x$, $x \sim y \Leftrightarrow y \sim x$ and $x \sim y, y \sim z \Rightarrow x \sim z$ for any x, y, z. The relation $\sim$ divides $\mathbb{R}$ into disjoint nonempty sets, where each set is of the form $\{y : y \sim x\}$ for some x. Let V be a selector for that partition. Then

- $(q + V) \cap V = \emptyset$ for every rational $q \neq 0$; otherwise, if $x \in (q + V) \cap V$ then $x = y + q$ for some $x, y \in V$, which gives $x \sim y, x \neq y$, a contradiction.
- $\bigcup_{q \in \mathbb{Q}} (q + V) = \mathbb{R}$.
- We can assume that $V \subseteq [0, 1)$. Then

$$[0, 1) \subseteq \bigcup_{q \in \mathbb{Q} \cap [-1,1)} (q + V) \subseteq [-1, 2).$$

Is Axiom of Choice controversial?

Banach-Tarski paradox

The ball of radius 1 (in $\mathbb{R}^3$) can be, by AC, decomposed into 5 pieces. Using those sets one can, using rotations and translations, form two balls of radius 1.

It follows that 1=2 so there must be something wrong with AC.
. . . Or with you intuition concerning the volume. Why do you assume that you can measure the volume of every set in $\mathbb{R}^3$?

Thank yor for your attention!

David Hilbert:

> *No one shall expel us from the Paradise that Cantor has created.*

Georg Cantor:

> *The essence of mathematics lies entirely in its freedom.*

Basic set-theoretic techniques in logic
Part V, Infinite Games

Benedikt Löwe
Universiteit van Amsterdam
Grzegorz Plebanek
Uniwersytet Wrocławski

ESSLLI 2011, Ljubljana, Slovenia

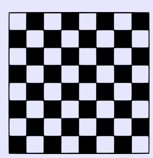
Let's play chess...

Ernst Zermelo (1871–1953)

Ernst Zermelo, Über eine Anwendung der Mengenlehre auf die Theorie des Schachspiels,

What is a chess configuration?

- There are 64 squares on a chess board:



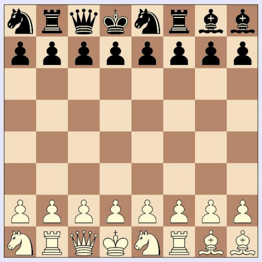
- There are 13 possible ways to fill a square.
  X ♙ ♟ ♖ ♜ ♘ ♞ ♗ ♝ ♕ ♛ ♔ ♚
- Thus, there are at most 64^{13} possible configurations of chess. Most of them are illegal.

Chess as a mathematical object (1).

We can think about playing chess as playing a sequence of natural numbers that stand for these at most 64^{13} configurations:

$$n_0 \xrightarrow{\text{WHITE}} n_1 \xrightarrow{\text{BLACK}} n_2 \xrightarrow{\text{WHITE}} n_3 \rightarrow \ldots$$

where n_0 corresponds to



and each of the other numbers represents something like

   or .

Chess as a mathematical object (2).

We can think of the entire game tree to be the infinite 64^{13}-branching tree (i.e., a finitely branching tree). There are a number of different types of nodes in this tree:

1. Nodes that end in an illegal position,
2. nodes in which WHITE has lost,
3. nodes in which BLACK has lost,
4. nodes that determine that the game is a draw,
5. nodes in which neither of the following cases has occurred.

If the same configuration occurs twice for the same player, then a game is counted as a draw. So, any sequence of $2 \cdot 64^{13} + 1$ moves in chess in which neither of 1., 2., or 3. has occurred is a draw. That means that we can cut off the tree at $2 \cdot 64^{13} + 1$ and obtain a finite tree.

Chess as a mathematical object (3).

Let's prune the tree:

1. Nodes that end in an illegal position,
2. nodes in which WHITE has lost,
3. nodes in which BLACK has lost,
4. nodes that determine that the game is a draw,
5. nodes in which neither of the following cases has occurred.

Step 1. If the last position of a node p is an illegal position, search backwards to the root and find the first position p^* in that sequence that is illegal. Cut off the tree after that node.

Step 2. If p is a node in which WHITE or BLACK has lost or the game is a draw, cut off the tree after that node.

In the resulting tree T, the terminal nodes are exactly those in which it is determined whether WHITE won, BLACK won or the game is a draw.

Chess as a mathematical object (4).

Define $\mathrm{depth}(p)$ to be the length of the longest path from p to a terminal node. Note that for every $p \in T$, $\mathrm{depth}(p) \leq 2 \cdot 64^{13} + 1$. Note furthermore that a node p is terminal if and only if $\mathrm{depth}(p) = 0$.

Define a function label by recursion:

- If p is terminal, and t is a loss for WHITE, then let $\mathrm{label}(p) = $ BLACK.
- If p is terminal, and t is a loss for BLACK, then let $\mathrm{label}(p) = $ WHITE.
- If p is terminal, and t is a draw, then let $\mathrm{label}(p) = $ DRAW.
- If p is terminal, and the last position is illegal, then if the last move was for WHITE, then let $\mathrm{label}(p) = $ BLACK; if the last move was for BLACK, then let $\mathrm{label}(p) = $ WHITE.

This defines label on all nodes of depth 0. The label determines the outcome of the game if the game reaches that node.

Chess as a mathematical object (5).

Suppose label is define for all nodes of depth i. Let p be a node of depth $i+1$ where WHITE has to move. All successors of p already have labels.

Case 1. If at least one of them is labelled WHITE, then label p WHITE as well.

Case 2. If none of them is labelled WHITE, but at least one is labelled DRAW, then label p DRAW.

Case 3. If all of them are labelled BLACK, then label p BLACK.

Now let p be a node of depth $i+1$ where BLACK has to move.

Case 1. If at least one of them is labelled BLACK, then label p BLACK as well.

Case 2. If none of them is labelled BLACK, but at least one is labelled DRAW, then label p DRAW.

Case 3. If all of them are labelled WHITE, then label p WHITE.

By the recursion principle, label is a total function on T, and thus the root has a label.

Chess as a mathematical object (6).

Theorem. If the root has label WHITE, then WHITE has a winning strategy; if the root has label DRAW, then both players have a drawing strategy; if the root has label BLACK, then BLACK has a winning strategy.

Corollary. One of the following three cases holds:

1. WHITE has a winning strategy in chess,
2. BLACK has a winning strategy in chess,
3. both players have a drawing strategy in chess.

Of course, to this day, it is not known which of the three cases holds.

Infinite games.

We fix an arbitrary set X of possible moves. We have two players, I and II. I plays in the even rounds (0,2,4,...) and II plays in the odd rounds (1,3,5,7,...).

Together, they produce an infinite sequence

$$x_0, x_1, x_2, x_3, x_4, \ldots$$

i.e., a function $x : \mathbb{N} \to X$.

We fix a payoff function $A : X^{\mathbb{N}} \to \{\mathrm{I}, \mathrm{II}, \textsc{draw}\}$.

Combinatorially, think of this as the infinitely long X-branching tree T_X in which the two players move by alternatingly producing an infinite branch.

Chess as a special case.

Let $X = 64^{13}$, and consider the finite pruned tree we constructed before as $T_{\mathrm{Chess}} \subseteq T_X$. Suppose that x is an infinite branch through T_X. Then it passes through a unique terminal node of T_{Chess}.

Now define

$$A_{\mathrm{Chess}}(x) := \mathrm{label}(t_x).$$

Some simplifying conventions.

From now on, we'll let $X = \mathbb{N}$, and we'll ignore the option $\textsc{draw}$. That means in our games, exactly one of the players wins.

This means that we do not really need a payoff function anymore, but can instead use a payoff set $A \subseteq \mathbb{N}^{\mathbb{N}}$, interpreting an outcome

$$x \in A$$

as a win for player I and an outcome

$$x \notin A$$

as a win for player II.

Strategies.

Let T^{I} be the set of nodes of $T_X = T_{\mathbb{N}}$ of even length; in other words, those nodes where player I has to play. Similarly, let T^{II} be the set of nodes of $T_X = T_{\mathbb{N}}$ of odd length.

A strategy for player I is a function $\sigma : T^{\mathrm{I}} \to \mathbb{N}$, and a strategy for player II is a function $\tau : T^{\mathrm{II}} \to \mathbb{N}$.

If σ and τ are such strategies, we can let them play against each other and recursively define $\sigma * \tau$:

$$(\sigma * \tau)(2n) := \sigma((\sigma * \tau)\restriction 2n)$$
$$(\sigma * \tau)(2n+1) := \tau((\sigma * \tau)\restriction 2n+1)$$

A strategy σ for player I is winning if for all τ, we have $\sigma * \tau \in A$.

A strategy τ for player II is winning if for all σ, we have $\sigma * \tau \notin A$.

Strategies as trees (1).

A strategy σ defines a tree $T_\sigma \subseteq T_{\mathbb{N}}$ by the following recursive definition:

- if $s \in T^{\mathrm{I}} \cap T_\sigma$, then $s\sigma(s) \in T_\sigma$;
- if $s \in T^{\mathrm{II}} \cap T_\sigma$, then $sx \in T_\sigma$ for any $x \in \mathbb{N}$.

If τ is any strategy for player II, then $\sigma * \tau$ is a branch through T_σ.

We can now reformulate: σ is winning for I if every branch through T_σ is in A.

Let's investigate T_σ. Let Z_σ be its set of branches. We'll show that $|Z_\sigma| = \mathfrak{c}$.

Strategies as trees (2).

Proof. It's easy to see that $|\mathbb{N}^{\mathbb{N}}| = \mathfrak{c}$. Since $Z_\sigma \subseteq \mathbb{N}^{\mathbb{N}}$, we get $|Z_\sigma| \leq \mathfrak{c}$.

For the other direction, we only need to produce an injection from the power set of $\mathbb{N}$ to Z_σ. As before, we identify the power set of $\mathbb{N}$ with $\{0,1\}^{\mathbb{N}}$ by

$$M \mapsto x_M$$

with

$$x_M(n) = \begin{cases} 1 & \text{if } n \in M, \\ 0 & \text{otherwise.} \end{cases}$$

We define a strategy for player II as follows. If $s \in T^{\mathrm{II}}$ and the length of s is $2n+1$, we let

$$\tau_M(s) := x_M(n).$$

Now consider $\sigma * \tau_M$. Clearly, if $M \neq M'$, then $\sigma * \tau_M \neq \sigma * \tau_{M'}$. So,

$$M \mapsto \sigma * \tau_M$$

is an injection from the power set of $\mathbb{N}$ into Z_σ. q.e.d.

Strategies as trees (3).

Using the same technique, you can show that there are exactly $\mathfrak{c}$ many strategies.

Proof. Homework.

Corollary.

1. If A is countable, then I cannot have a winning strategy in the game with payoff set A.
2. If the complement of A is countable, then II cannot have a winning strategy in the game with payoff set A.

An application (?)

Theorem (Morton Davis). For each $A \subseteq \mathbb{N}^{\mathbb{N}}$ there is a game G^*_A such that

1. If I has a winning strategy in G^*_A, then $|A| = \mathfrak{c}$.
2. If II has a winning strategy in G^*_A, then $|A| \leq \aleph_0$.

Corollary. If we can show that all games have a winning strategy for one of the two players, then the Continuum Hypothesis holds.

Existence of non-determined sets.

Theorem. The Axiom of Choice implies the existence of a set such that neither of the players has a winning strategy.

Proof. We had seen that there are $\mathfrak{c}$ many strategies. Use the Axiom of Choice to list them in a wellordered list $\{\sigma_\alpha \; ; \; \alpha < \mathfrak{c}\}$. We also saw that for each of these strategies σ_α, its set of branches Z_α has $\mathfrak{c}$ many elements.

Recursively define disjoint sets A and B such that each strategy contains an element of A and B. Then there can be no winning strategy for either play in the game with payoff set A. q.e.d.

Gale-Stewart theorem.

A set A is called finite horizon if there is a set $W \in T_{\mathbb{N}}$ such that

$$x \in A \text{ if and only if } \exists p \in W (x \text{ passes through } p).$$

Theorem. For every finite horizon game there is either a winning strategy for player I or for player II.

Isn't this just like in the chess example?

> *You prune the tree after the nodes $p \in W$, then these nodes become terminal nodes, and you label them with I. Then you run the recursion and if the root gets label I, then I has a winning strategy; if not then II has a winning strategy.*

Well, it's not so simple since we now have infinitely branching trees.