How do you prove that something is unprovable?

A. Andretta

Dipartimento di Matematica
Università di Torino

Torino 28 April 2014

Cantor's continuum problem

Two sets A and B have the same cardinality if there is a bijection between them, in symbols $A \approx B$.

Example

$\mathbb{N}$, $\mathbb{Q}$, $\{r \in \mathbb{R} \mid r$ is algebraic$\}$, ... have the same cardinality.

Theorem (Cantor)

A and $\mathscr{P}(A)$ have distinct cardinalities.
In particular $\mathbb{N}$ and $\mathbb{R} \approx \mathscr{P}(\mathbb{N})$ have distinct cardinalities.

Cantor's continuum problem

Is it true that every infinite subset of $\mathbb{R}$ is either in bijection with $\mathbb{N}$ or with $\mathbb{R}$?

Ordinals and cardinals

Lower case greek letters like $\alpha, \beta, \gamma, \ldots$ denote **ordinals.**
$\kappa, \lambda, \ldots$ usually denote infinite **cardinals** i.e. ordinals that are not in bijection with any smaller ordinal.
ω is the least infinite ordinal, and it is a cardinal.
$\aleph_0 = \omega$ is the cardinality on $\mathbb{N}$.
$\aleph_1 = \omega_1$ is the least cardinal $> \aleph_0$. More generally: $\aleph_{\alpha+1}$ is the least cardinal $> \aleph_\alpha$.
κ^λ is the size of ${}^\lambda\kappa \stackrel{\text{def}}{=} \{f \mid f\colon \lambda \to \kappa\}$.

Independence

Cantor's theorem, restated

$2^\kappa > \kappa$

Cantor's continuum problem, restated

Is $2^{\aleph_0} = \aleph_1$?

CH is the statement $2^{\aleph_0} = \aleph_1$ or equivalently "every subset of $\mathbb{R}$ is either countable, or it is in bijection with $\mathbb{R}$".

CH cannot be proved nor can be disproved from the usual axioms of set theory!

By the usual axioms of set theory we mean ZFC, the Zermelo-Frænkel axiom system together the Axiom of Choice. It is a set of axioms in first order logic…

First order logic

A **first order language** consists of

- logical symbols: $\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, $\exists$, $\forall$
- variables: $x, y, z, \ldots$
- nonlogical symbols (predicate symbols, function symbols)

The language of set theory is the first order language with only one nonlogical binary relational symbol $\in$.

Formulæ will be denoted with $\varphi, \psi, \ldots$. A **sentence** is a formula without free variables.

Given a set of sentences Σ, a **derivation** from Σ is a finite sequence $\langle \varphi_0, \ldots, \varphi_n \rangle$ where each φ_i is either

- an element of Σ, or else
- a logical axiom, or else
- it can be obtained from the φ_j ($j < i$) by means of the logical rules.

Logical axioms and logical rules

Logical axioms

- any tautology
- $\varphi[y/x] \Rightarrow \exists x \varphi$
- $x = x$,
- $x = y \Rightarrow y = x$,
- $x = y \wedge y = z \Rightarrow x = z$,
- $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \wedge \varphi(x_1, \ldots, x_n) \Rightarrow \varphi(y_1, \ldots, y_n)$.

Logical rules

Modus ponens: from φ and $\varphi \Rightarrow \psi$ we can derive ψ;

Universal-quantification rule: if x is not free in φ, then from $\varphi \Rightarrow \psi$ we can derive $\varphi \Rightarrow \forall x \psi$.

Derivations and theorems

If Σ is a set of sentences in a first order language and $\langle \varphi_0, \dots, \varphi_n \rangle$ is a derivation from Σ, then $\langle \varphi_0, \dots, \varphi_m \rangle$ is a derivation from Σ, for all $m < n$.

If $\langle \varphi_0, \dots, \varphi_n \rangle$ is a derivation from Σ, then φ_n is a **theorem** of Σ, in symbols

$$\Sigma \vdash \varphi_n$$

If a mathematical theory (like set theory) is axiomatized in a first order language, then any usual mathematical argument can in principle be transformed into a derivation.

Our goal

Show that ZFC $\nvdash$ CH and ZFC $\nvdash \neg$CH

Axioms of ZFC — first group

Axiom of Extensionality

Two sets x and y are equal if they have exactly the same elements:
$\forall x \forall y\, (\forall z (z \in x \Leftrightarrow z \in y) \Rightarrow x = y)$.

Axiom of Pairing

Given two sets x and y there is always a set z to which the belong:
$\forall x \forall y \exists z\, (x \in z \wedge y \in z)$.

Axiom of Union

Given x there is a y such that all elements of x are subsets of y:
$\forall x \exists y \forall z\, (z \in x \Rightarrow z \subseteq y)$.

Axiom of Power set

Given a set x there is a set y to which all subsets of x belong:
$\forall x \exists y \forall z\, (z \subseteq x \Rightarrow z \in y)$.

Axioms of set theory — second group

Axiom of Infinity

There is a set x containing the empty set, and closed under the operation $y \mapsto \mathbf{S}(y) \stackrel{\text{def}}{=} y \cup \{y\}$:
$\exists x\,(\emptyset \in x \wedge \forall y\,(y \in x \Rightarrow \mathbf{S}(y) \in x))$.

Axiom of Foundation

Every nonempty set x has an element y which is disjoint from x:
$\forall x \neq \emptyset\, \exists y \in x\,(y \cap x = \emptyset)$.

Axiom of Choice

Given a family A of sets there is a function f such that $\mathrm{dom}(f) = A$ and $f(x) \in x$, for all $\emptyset \neq x \in A$:
$\forall A \exists f\,(f \text{ is a function } \wedge \mathrm{dom}(f) = A \wedge \forall x \in A\ (x \neq \emptyset \Rightarrow f(x) \in x))$.

Axioms of ZFC — third group

Axiom of Separation

Given a set B and a property $\varphi(x)$ we can construct the set A of all elements of B that satisfy φ:
for each formula $\varphi(x, B, y_1, \ldots, y_n)$ with x free, and A distinct from $x, B, y_1, \ldots, y_n$, $\forall y_1 \ldots \forall y_n \forall B \exists A \forall x\, (x \in A \Leftrightarrow x \in B \wedge \varphi(x, B, y_1, \ldots, y_n))$.

Axiom of Replacement

Given an operation $x \mapsto y$ defined on a set A there is a set B which is the image of A under such an operation:
for each formula $\varphi(x, y, A, z_1, \ldots, z_n)$ and each variable B distinct from $x, y, A, z_1, \ldots, z_n$,

$$\forall A \forall z_1 \ldots \forall z_n\, (\forall x\, (x \in A \Rightarrow \exists! y \varphi(x, y, A, z_1, \ldots, z_n)) \Rightarrow \\ \exists B \forall y\, (y \in B \Leftrightarrow \exists x\, (x \in A \wedge \varphi(x, y, A, z_1, \ldots, z_n)))) .$$

A bit of history. . .

Kurt Gödel in 1938 introduced the notion of constructible set and showed that CH cannot be refuted from ZFC, i.e. ZFC $\nvdash \neg$CH.
Paul Cohen in 1963 introduced the method of forcing and showed that CH cannot be proved from ZFC, i.e. ZFC $\nvdash$ CH. Forcing can also be used to show ZFC $\nvdash \neg$CH.
Dana Scott and Robert Solovay soon after found an equivalent, simpler, reformulation of forcing in terms of boolean valued models.

Reference

John Bell, *Set Theory: Boolean-Valued Models and Independence Proofs*, Oxford University Press.

Goal: show that ZFC $\nvdash$ CH and ZFC $\nvdash \neg$CH

Idea

attach labels, say $\mathbf{0}$ and $\mathbf{1}$, to each sentence so that every axiom of ZFC and every logical axiom is labelled $\mathbf{1}$, and the logical rules preserve label $\mathbf{1}$, yet CH is labelled $\mathbf{0}$.
Similarly for $\neg$CH.

The set of labels will be a **boolean algebra**, i.e. a set $\mathbf{B}$ with two binary operations $\curlywedge$ and $\curlyvee$, a unary operation *, and two distinguished elements $\mathbf{0} \neq \mathbf{1}$ such that

- $\curlywedge$ and $\curlyvee$ are commutative and associative, and distributive with respect to each other:
$$(x \curlyvee y) \curlywedge z = (x \curlywedge z) \curlyvee (y \curlywedge z) \quad \text{and} \quad (x \curlywedge y) \curlyvee z = (x \curlyvee z) \curlywedge (y \curlyvee z)$$
- $\forall x\,(x \curlyvee x^* = \mathbf{1})$, $\forall x\,(x \curlywedge x^* = \mathbf{0})$, $\forall x\,(x \curlyvee \mathbf{0} = x)$ and $\forall x\,(x \curlywedge \mathbf{1} = x)$.

A short digression: boolean algebras

Examples

- $\{\mathbf{0}, \mathbf{1}\}$ is the simplest example of a boolean algebra.
- $\mathscr{P}(X)$ is a boolean algebra: $A \curlywedge B = A \cap B$, $A \curlyvee B = A \cup B$, $A^* = X \setminus A = \complement A$, and $\mathbf{1} = X$ and $\mathbf{0} = \emptyset$.
- Every boolean algebra $\mathbf{B}$ is isomorphic to subalgebra of some $\mathscr{P}(X)$, i.e. it is of the form $\mathcal{F} \subseteq \mathscr{P}(X)$, with $\mathcal{F}$ closed under unions, intersections, and complements.

$\mathscr{P}(X)$ is a partially ordered set under $\subseteq$, and

$$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B.$$

Similarly in any boolean algebra we define the partial $x \leq y$ iff $x \curlywedge y = x$ or equivalently, iff $x \curlyvee y = y$.
$\mathbf{0}$ is the minimum, and $\mathbf{1}$ is the maximum.

The plot thickens...

Recall that we want to replace classical truth by probabilistic truth by labeling sentences with elements elements of a boolean algebra $\mathbf{B}$, in such a way that every axiom of ZFC and every logical axiom is labelled $\mathbf{1}$, and the logical rules preserve label $\mathbf{1}$, yet CH is labelled $\mathbf{0}$. Unfortunately, a derivation contains formulæ that are not sentences, so in order to carry-out our plan, we need to label formulæ with free variables... This in turn suggests to

Replace sets with probabilistic sets

Every set A can be identified with its characteristic function $\chi_A : A' \to \{\mathbf{0}, \mathbf{1}\}$, with A' any superset of A. So the generalization should be some function taking values in $\mathbf{B}$...

Boolean valued models

Fix $\mathbf{B}$ a boolean algebra, and construct a class of sets $\mathrm{V}^{(\mathbf{B})}$ of all functions taking values in $\mathbf{B}$, whose domain is made-up of functions taking values in $\mathbf{B}$, whose domain is made-up of functions taking values in $\mathbf{B}$, ...

More precisely

$$\mathrm{V}^{(\mathbf{B})} = \bigcup_{\alpha \in \mathrm{Ord}} \mathrm{V}_{\alpha}^{(\mathbf{B})},$$

where

- $\mathrm{V}_0^{(\mathbf{B})} = \emptyset$
- $\mathrm{V}_{\alpha+1}^{(\mathbf{B})} = \{u \mid u$ is a function $\wedge \operatorname{dom}(u) \subseteq \mathrm{V}_{\alpha}^{(\mathbf{B})} \wedge \operatorname{ran}(u) \subseteq \mathbf{B}\}$.
- $\mathrm{V}_{\lambda}^{(\mathbf{B})} = \bigcup_{\alpha<\lambda} \mathrm{V}_{\alpha}^{(\mathbf{B})}$, for λ limit.

Complete boolean algebras

Although $V^{(\mathbf{B})}$ makes sense for *any* boolean algebra, for technical reasons we must restrict ourselves to **complete boolean algebras** $\mathbf{B}$, i.e. such that every $X \subseteq \mathbf{B}$ has a least upper bound $b \in \mathbf{B}$, that is

$$\forall x \in X \ (x \leq b) \curlywedge \forall c \in \mathbf{B} \ [\forall x \in X \ (x \leq c) \Rightarrow b \leq c] .$$

The element b is denoted either with $\bigvee X$ or with $\sup X$.

Fact

$\mathbf{B}$ is complete iff every $X \subseteq \mathbf{B}$ has a greatest lower bound in $\mathbf{B}$, denoted by $\bigwedge X$ or $\inf X$.

Note that $\mathbf{1} = \bigvee \mathbf{B}$ and $\mathbf{0} = \bigwedge \mathbf{B}$.

Examples

Every *finite* boolean algebra is complete.
$\mathscr{P}(A)$ is a complete boolean algebra.

Boolean truth in $V^{(\mathbf{B})}$

We shall define the $\mathbf{B}$-probability that φ holds at $u_1, \dots, u_n \in V^{(\mathbf{B})}$,

$$[\![\varphi(u_1, \dots, u_n)]\!]_{\mathbf{B}} = [\![\varphi(u_1, \dots, u_n)]\!] \in \mathbf{B}.$$

Assuming this is done for the atomic formulæ (difficult), the definition is by induction on the complexity of φ:

$$\begin{aligned}
[\![\neg\varphi(u_1, \dots, u_n)]\!] &= [\![\varphi(u_1, \dots, u_n)]\!]^* \\
[\![\varphi(u_1, \dots, u_n) \wedge \psi(u_1, \dots, u_n)]\!] &= [\![\varphi(u_1, \dots, u_n)]\!] \curlywedge [\![\psi(u_1, \dots, u_n)]\!] \\
[\![\varphi(u_1, \dots, u_n) \vee \psi(u_1, \dots, u_n)]\!] &= [\![\varphi(u_1, \dots, u_n)]\!] \curlyvee [\![\psi(u_1, \dots, u_n)]\!] \\
[\![\varphi(u_1, \dots, u_n) \Rightarrow \psi(u_1, \dots, u_n)]\!] &= [\![\varphi(u_1, \dots, u_n)]\!]^* \curlyvee [\![\psi(u_1, \dots, u_n)]\!] \\
[\![\varphi(u_1, \dots, u_n) \Leftrightarrow \psi(u_1, \dots, u_n)]\!] &= [\![\varphi(u_1, \dots, u_n) \Rightarrow \psi(u_1, \dots, u_n)]\!] \\
&\qquad \curlywedge [\![\psi(u_1, \dots, u_n) \Rightarrow \varphi(u_1, \dots, u_n)]\!] \\
[\![\exists x\varphi(x, u_1, \dots, u_n)]\!] &= \bigvee\{[\![\varphi(v, u_1, \dots, u_n)]\!] \mid v \in V^{(\mathbf{B})}\} \\
[\![\forall x\varphi(x, u_1, \dots, u_n)]\!] &= \bigwedge\{[\![\varphi(v, u_1, \dots, u_n)]\!] \mid v \in V^{(\mathbf{B})}\}.
\end{aligned}$$

Boolean truth in $V^{(\mathbf{B})}$

Atomic formulæ

If φ is either $x \in y$ or $x = y$:

$$
\begin{aligned}
[\![u \in v]\!] &= \bigvee_{z \in \mathrm{dom}(v)} \left(v(z) \curlywedge [\![z = u]\!] \right) \\
[\![u = v]\!] &= \bigwedge_{z \in \mathrm{dom}(u)} \left(u(z)^* \curlyvee [\![z \in v]\!] \right) \curlywedge \bigwedge_{z \in \mathrm{dom}(v)} \left(v(z)^* \curlyvee [\![z \in u]\!] \right) \\
&= [\![\forall x \, (x \in u \Rightarrow x \in z) \wedge \forall x \, (x \in v \Rightarrow x \in u)]\!]
\end{aligned}
$$

The value $[\![\varphi(u_1, \ldots, u_n)]\!]$ depends on $u_1, \ldots, u_n$, while $[\![\sigma]\!]$ does not, for σ a sentence.

The plan…

Main technical fact

- if $\varphi(x_1, \dots, x_n)$ is a logical axiom, then $[\![\varphi(u_1, \dots, u_n)]\!] = \mathbf{1}$,
- if σ is an axiom of ZFC, then $[\![\sigma]\!] = \mathbf{1}$,
- if $\langle \varphi_0, \dots, \varphi_m \rangle$ is a derivation in ZFC and $(x_1, \dots, x_n)$ are the variables occurring free in any one of the φ_i, then $[\![\varphi_i(u_1, \dots, u_n)]\!] = \mathbf{1}$ for all $u_1, \dots, u_n \in \mathrm{V}^{(\mathbf{B})}$.

Corollary

If ZFC $\vdash \sigma$, *then* $[\![\sigma]\!] = \mathbf{1}$.

It all boils down to…

…find complete boolean algebras $\mathbf{B}_1$ and $\mathbf{B}_2$ such that $[\![\mathrm{CH}]\!]_{\mathbf{B}_1} \neq \mathbf{1}$, and $[\![\neg\mathrm{CH}]\!]_{\mathbf{B}_2} \neq \mathbf{1}$.

Defined objects

CH says: $\exists f\,(f$ is a function from ω_1 onto $\mathscr{P}(\omega))$.
$\neg$CH says: $\exists f\,(f$ is an injective function from ω_2 into $\mathscr{P}(\omega))$.
These are not, strictly speaking, formulæ in the language of set theory!
We need to understand how "f is a function", "ω_1" and "$\mathscr{P}(\omega)$" look in $\mathrm{V}^{(\mathbf{B})}$. For each set x define $\check{x} \in \mathrm{V}^{(\mathbf{B})}$ as follows

$$\check{x} \colon \{\check{y} \mid y \in x\} \to \mathbf{B}, \qquad \check{x}(\check{y}) = \mathbf{1}.$$

Then $[\![\check{y} \in \check{x}]\!] = \mathbf{1} \Leftrightarrow y \in x$ and $[\![\check{y} = \check{x}]\!] = \mathbf{1} \Leftrightarrow y = x$.

Questions

Fix a complete boolean algebra $\mathbf{B}$.
If $x = \omega$ is it true that $[\![\check{x}$ is the least infinite ordinal$]\!]$? YES!
If $x = \mathscr{P}(\omega)$ is it true that $[\![\check{x}$ is the collection of all subsets of $\omega]\!]$? If $x = \omega_1$ is it true that $[\![\check{x}$ is the least uncountable cardinal$]\!]$? MAYBE, it depends on $\mathbf{B}$!

More on complete boolean algebras

If X is a topological space, then $U \subseteq X$ is regular open just in case $U = \mathrm{Int}(\mathrm{Cl}(U))$, and $\mathbf{RO}(X)$ is the family of all regular open sets. It is a complete boolean algebra:

$$\begin{aligned} U \curlywedge V &= U \cap V \\ U \curlyvee V &= \mathrm{Int}(\mathrm{Cl}(U \cup V)) \\ U^* &= \mathrm{Int}(X \setminus U). \end{aligned}$$

Any complete boolean algebra is isomorphic to $\mathbf{RO}(X)$ for some suitable topological space X.

The consistency of $\neg$CH

Let κ be an infinite cardinal. Endow tha set $\prod_{i\in\kappa}\{0,1\}$ with the product topology, taking $\{0,1\}$ to be discrete. Let $\mathbf{B}$ be the boolean algebra of its regular open sets.

- If $x = \omega_n$ then $[\![\check{x} = \omega_n]\!] = \mathbf{1}$, for any n.
- If $x = \mathscr{P}(\omega)$, then $[\![\check{x} \neq \mathscr{P}(\omega)]\!] = \mathbf{1}$.
- If $\kappa \geq \omega_2$ then
  $[\![\exists f\,(f$ is an injective function from ω_2 into $\mathscr{P}(\omega))]\!] = \mathbf{1}$.

Thus by taking $\kappa \geq \omega_2$ we get a complete boolean algebra $\mathbf{B}$ such that $[\![\neg\text{CH}]\!]_{\mathbf{B}} = \mathbf{1}$.

The consistency of CH

Let κ, λ be infinite cardinals. Endow the set $\prod_{i\in\kappa}\lambda$ with the topology generated by all sets

$$\prod_{i\in I}\{\alpha_i\} \times \prod_{i\in\kappa\setminus I}\lambda$$

with I countable and $\alpha_i \in \lambda$. Let $\mathbf{B}$ be the regular open algebra of this topological space.

- If $x = \mathscr{P}(\omega)$, then $[\![\check{x} = \mathscr{P}(\omega)]\!] = \mathbf{1}$.
- If $x = \omega_1$ then $[\![\check{x} = \omega_1]\!] = \mathbf{1}$.
- If $\kappa = \omega_1$ and $\lambda = 2^{\aleph_0}$ then $[\![\exists f\,(f$ is an surjective function from ω_1 onto $\mathscr{P}(\omega))]\!] = \mathbf{1}$.

Thus by taking $\kappa = \omega_1$ and $\lambda = 2^{\aleph_0}$ we get a complete boolean algebra $\mathbf{B}$ such that $[\![\mathrm{CH}]\!]_{\mathbf{B}} = \mathbf{1}$.