Independence in set theory

Jakob Everling

8. Juli 2020

Contents

Introduction

In this talk, we want to examine the notion of provability. We will attempt to answer the following questions:

- What exactly does it mean to prove something?
- Can every statement be proved or disproved?
- How can we show whether a specific statement can be proven?

Logic systems

To specify a formal approach to mathematics, we need:

- A language, defining what a „mathematical statement“ is.
- Some logical axioms, which are formulae we define to be true.
- Some rules of deduction, to define which steps are allowed in a proof.

Most modern mathematics is done using:

- The language of first-order predicate logic.
- Some standard logical axioms such as $\varphi \to \varphi \vee \psi$.
- The Modus Ponens: From φ and $\varphi \to \psi$, we can conclude ψ.

We will use this system throughout the rest of the talk.

Proofs

Definition

Let Γ be a set of formulae. A proof of φ from Γ is a finite string of formulae $\varphi_0, \ldots, \varphi_n = \varphi$ such that for every φ_i, at least one of the following holds:

- φ_i is a logical axiom,
- $\varphi_i \in \Gamma$,
- φ_i follows from some of the φ_j ($j < i$) using one of the rules of deduction.

If such a proof exists, we write $\Gamma \vdash \varphi$.

Definition

φ is independent of Γ if $\Gamma \nvdash \varphi$ and $\Gamma \nvdash \neg\varphi$.

Properties of logical systems

The following properties are very desirable in a logical system:

Consistency

A system of logic is consistent if it does not produce a contradiction, so there is no formula φ such that φ and $\neg\varphi$ can be proven.

Completeness

A system of logic is complete if every sentence can be proved or disproved.

Gödel's Incompleteness theorems

Kurt Gödel showed in 1931 that we can't have both (see [1]):

Incompleteness Theorems

Let S be a system of logic strong enough to describe the arithmetic of the natural numbers.

1. S is either inconsistent or incomplete.
2. S cannot prove its own consistency.

Note: The prerequisite „strong enough to describe the natural numbers" is made precise in Gödel's work [1].

What Incompleteness means

Applying the first Incompleteness Theorem to ZF/ZFC and assuming consistency, we get

Standard mathematics is incomplete

There are mathematical statements that cannot be proved or disproved using standard mathematical reasoning.

Note: To show this, Gödel found a way to mathematically write the statement „*I am not provable*“. This „pathological“ example was seen by some to be inconsequential to real mathematics. We will show some more mathematically interesting statements that are independent of ZFC.

The most important example

Let $\aleph_0$ denote countable infinity and let $\mathfrak{c} = |\mathbb{R}|$ be the cardinality of the real numbers. Georg Cantor showed in 1874 that $\aleph_0 < \mathfrak{c}$ (see [2]).
Let $\aleph_1$ denote the smallest infinity larger than $\aleph_0$. Since $\aleph_0 < \mathfrak{c}$, we have $\aleph_1 \leq \mathfrak{c}$. Does $\geq$ also hold?
The *Continuum Hypothesis* states that:

Continuum Hypothesis (CH)

$\aleph_1 = \mathfrak{c}$.

In other words: For every uncountable $X \subseteq \mathbb{R}$ there is a bijection $X \to \mathbb{R}$.
Deciding CH was the first of Hilbert's 23 problems presented in 1900. Paul Cohen showed in 1963 that CH is independent of ZFC (see [3], [4]).

Example: Commutative Algebra

A module P over a ring R is projective if there is a module Q such that $P \oplus Q$ is free. The projective dimension $\mathrm{pd}_R(M)$ of a module M is the smallest n such that there exists an exact sequence $0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$ with P_i projective.

Example

Let $R = \mathbb{C}[x, y, z]$ and $M = \mathbb{C}(x, y, z)$ as an R-module. Then

$$\mathrm{pd}_R(M) = \begin{cases} 2 & \text{if CH holds} \\ 3 & \text{if } \neg\text{CH holds.} \end{cases}$$

So the statements „$\mathrm{pd}_R(M) = 2$“ and „$\mathrm{pd}_R(M) = 3$“ are independent of ZFC.

Example: Measure Theory

A set $X \subseteq \mathbb{R}$ has strong measure zero if for every sequence $(a_n)_{n\in\mathbb{N}}$ of positive reals, there is a set of intervals $(I_n)_{n\in\mathbb{N}}$ such that

$$X \subseteq \bigcup_{n\in\mathbb{N}} I_n \quad \text{and} \quad \lambda(I_n) = a_n.$$

The following is independent of ZFC:

Borel conjecture

Every strong measure zero set is countable.

Note: This is a conjecture by Émile Borel. It is unrelated to a different *Borel conjecture* in geometric topology named for Armand Borel.

Example: Analysis

Reminder

Let A be a $\mathbb{C}$-algebra. A norm on A is a map $p : A \to \mathbb{R}$ such that

- $\forall a \in A \setminus \{0\} : p(a) > 0$
- $\forall a \in A, z \in \mathbb{C} : p(za) = |z|p(a)$
- $\forall a, b \in A : p(a + b) \leq p(a) + p(b)$
- $\forall a, b \in A : p(ab) \leq p(a)p(b)$

Two norms p, q on an algebra A are equivalent if

$$\exists c, C \in \mathbb{R}_{>0} : \forall a \in A : cp(a) \leq q(a) \leq Cp(a).$$

Equivalent norms induce the same topology on A.

Example: Analysis

Let X be a compact Hausdorff space and let $C(X, \mathbb{C})$ be the set of all continuous functions $X \to \mathbb{C}$, then $C(X, \mathbb{C})$ is a commutative $\mathbb{C}$-algebra wrt pointwise operations.

The uniform norm is the map

$$|\cdot|_X : C(X, \mathbb{C}) \to \mathbb{R},\ f \mapsto \sup\left\{|f(x)| : x \in X\right\}.$$

In 1948, Irving Kaplansky first thought about the following (see [5]):

Kaplansky's conjecture

Every norm on $C(X, \mathbb{C})$ is equivalent to the uniform norm $|\cdot|_X$.

This can be shown to be equivalent to

No discontinuous homomorphism (NDH)

Every homomorphism from $C(X, \mathbb{C})$ to any Banach algebra is continuous.

Robert Solovay proved in 1976 that this is independent from ZFC (see [5]).

Proving Independence

It is usually hard to prove independence results directly by talking about strings of formulae. The more successful approach has been finding models:

Definition

A model of set theory is a pair (M, E) such that M is a class and $E \subseteq M \times M$ is a relation on M.

Here, M can be understood as a „universe“ of objects, and E will be interpreted as $\in$. Formulae can be true or false within a model:

Example

Switzerland $\models$ „10% of people are millionaires.“
Note that „people“ and „millionaires“ are interpreted as „Swiss people“ and „people who own $\geq$ 1M Swiss Francs“.

Note: Different sources put the figure between 5% and 10%, see [6] and [7].

Truth within models

Let (M, E) be a model and let φ be a formula with free variables $x_1, \ldots, x_n$. Let $a_1, \ldots, a_n \in M$. To check whether M satisfies φ in $a_1, \ldots, a_n$:

- Replace every x_i in φ by a_i.
- Replace every $\in$ in φ by E.
- Restrict every quantifier to M: $\exists x$ becomes $\exists x \in M$.

If the resulting sentence is true, M satisfies φ in $a_1, \ldots, a_n$ and we write $M \models \varphi[a_1, \ldots, a_n]$.

Example

Let $M = \{1, 2, 3, 4\}$ and $E = \leq$. Then $(M, E) \models \exists x \forall y (y \in x)$, since the sentence $\exists x \in M : \forall y \in M : y \leq x$ is true.

Consistency and provability

Let Γ be a set of formulae.

Definition

Γ is consistent if there is no formula φ such that $\Gamma \vdash \varphi$ and $\Gamma \vdash \neg\varphi$.

Proposition

Let φ be a formula. If $\Gamma' := \Gamma \cup \{\neg\varphi\}$ is consistent, then $\Gamma \nvdash \varphi$.

Proof: Assume $\Gamma \vdash \varphi$, then the same proof also shows $\Gamma' \vdash \varphi$. Obviously $\Gamma' \vdash \neg\varphi$, so Γ' is inconsistent.

Soundness Theorem

Ex Falso Quodlibet

If Γ is inconsistent, then $\Gamma \vdash \varphi$ for every formula φ.

Soundness Theorem

Let Γ be a set of sentences. If there is a model (M, E) such that $(M, E) \models \Gamma$, then Γ is consistent.

Proof: Assume Γ is inconsistent, then $\Gamma \vdash \exists x : x \neq x$. Take a proof $\varphi_1, \ldots, \varphi_n$ of this. For any i, if φ_i is a logical axiom, any model believes it. If $\varphi_i \in \Gamma$ then $(M, E) \models \varphi_i$. If φ_i is concluded via Modus Ponens, then by induction hypothesis $(M, E) \models \varphi_j, \varphi_j \to \varphi_i$. Thus $(M, E) \models \varphi_i$.
In the end, $(M, E) \models \exists x : x \neq x$, so $\exists x \in M : x \neq x$. This is clearly not true, so Γ is consistent.

Proving Independence

Soundness Theorem

Let Γ be a set of sentences. If there is a model (M, E) such that $(M, E) \models \Gamma$, then Γ is consistent.

Corollary

Let Γ be a set of sentences. To show that a formula φ is independent of Γ, it suffices to construct models of $\Gamma \cup \{\varphi\}$ and $\Gamma \cup \{\neg\varphi\}$.

We also write $\Gamma + \varphi$ for $\Gamma \cup \{\varphi\}$.

Example

Let $\Gamma = \{\forall x \exists y (x \in y), \nexists x (x \in x)\}$ and $\varphi =$ „$\exists x \forall y (y \neq x \Rightarrow x \in y)$“.
Then $(\mathbb{N}, <) \models \Gamma + \varphi$ and $(\mathbb{Z}, <) \models \Gamma + \neg\varphi$, so φ is independent of Γ.

A sensible example

In 1938, Kurt Gödel showed that ZFC and CH are compatible (see [8]):

Constructible Universe

For any ordinal number α, define L_α by

- $L_0 := \emptyset$,
- $L_{\alpha+1} = \mathcal{D}(L_\alpha)$,
- $L_\gamma = \bigcup_{\alpha<\gamma} L_\alpha$ for limit ordinals γ,

where

$$\mathcal{D}(X) := \{\{y \in X \mid \varphi(y, z_0, \ldots, z_n)\} \mid \varphi \in \mathrm{Fml}, z_0, \ldots, z_n \in X\}.$$

Define $L := \bigcup_{\alpha \in \mathrm{Ord}} L_\alpha$.

Theorem

$(L, \in) \models \mathrm{ZFC} + \mathrm{CH}$.

Part of the Proof

Theorem

$(L, \in) \models \text{ZFC} + \text{CH}$.

Note: For any $x \in L_\alpha$, we have $x = \{y \mid y \in x\} \in L_{\alpha+1}$, and gerenally $x \in L_\beta$ for any $\beta > \alpha$. So $L_0 \subseteq L_1 \subseteq \ldots \subseteq L_\alpha \subseteq \ldots$

EmptySet: $\emptyset \in L$ since $\emptyset \in L_1$.

Extensionality: Take $x, y \in L$ with $\forall z \in L : z \in x \iff z \in y$. Since any $z \notin L$ lies in neither x nor y, this means $\forall z : z \in x \iff z \in y$, so $x = y$.

Pairing: For $x, y \in L$, take α, β such that $x \in L_\alpha, y \in L_\beta$. Then $\{x, y\} = \{z \mid z = x \vee z = y\} \in L_{\max(\alpha,\beta)+1}$.

The other ZF axioms can be technical, but they are not substantially harder. Choice and CH require more theory than we can do here.

Forcing

We have seen one technique to build a model: Start from an existing one and make it smaller.

Forcing is a technique to start from a model and make it larger.

Let M be a model of set theory with $M \models \text{ZFC}$. Given a specific set G, we will construct a model $M[G]$ with $M \subseteq M[G]$, $G \in M[G]$ and $M[G] \models \text{ZFC}$. Good choices of G will allow us to „force" some formulae to be true or false in $M[G]$.

Forcing

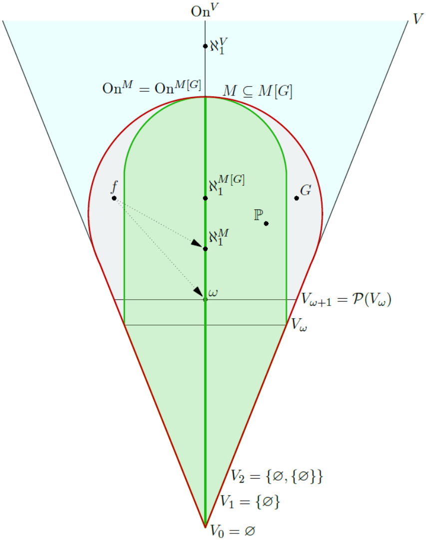


Illustration taken from [10]

Forcing posets

Always let $(\mathbb{P}, \leq)$ be a poset with largest element 1. Let M be a model.

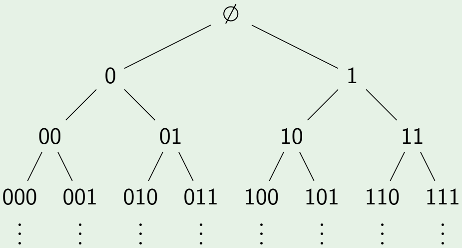
Definition

- Two elements $a, b \in \mathbb{P}$ are compatible if $\exists r \in \mathbb{P} : r \leq a, r \leq b$. In that case write $a \parallel b$, otherwise $a \perp b$.
- $F \subseteq \mathbb{P}$ is a filter iff $F \neq \emptyset$ and
  - $\forall a \in F, b \in \mathbb{P} : (b \geq a \Rightarrow b \in F)$ (F is upwards closed).
  - $\forall a, b \in F : a \parallel b$.
- $D \subseteq \mathbb{P}$ is dense iff $\forall p \in \mathbb{P} \exists r \in D : r \leq p$.
- $G \subseteq \mathbb{P}$ is generic iff $\forall D \subseteq \mathbb{P}$ dense : $G \cap D \neq \emptyset$.
- G is M-generic iff $\forall D \subseteq \mathbb{P}$ dense : $(D \in M \Rightarrow G \cap D \neq \emptyset)$.

Forcing posets

Example

Take $\mathbb{P} := 2^{<\omega} := \bigcup_{n\in\omega}(\{0,1\}^n)$:



- Elements are compatible iff they are comparable.
- The filters are the chains that contain $\emptyset$.
- For any filter F, $\mathbb{P} \setminus F$ is dense.
- There are no M-generic filters if $\mathcal{P}(\mathbb{P}) \subseteq M$.

Forcing posets

Example

Let I, J be any sets and define

$$\mathrm{Fn}(I,J) := \bigcup_{X \subseteq I \text{ finite}} \{f \mid f : X \to J\}.$$

Then $(\mathrm{Fn}(I,J), \supseteq)$ is a forcing poset.
f, g are compatible iff there is a function $h : I \to J$ with $h \supseteq f, g$.
For all $i \in I, j \in J$, $\{f \mid i \in \mathrm{dom}(f)\}$ and $\{f \mid j \in \mathrm{ran}(f)\}$ are dense.
The generic filters of $\mathrm{Fn}(I,J)$ correspond to functions $I \xrightarrow{\text{onto}} J$.

Existence of generic filters

We have seen: The existence of M-generic filters depends on the size of M.

Definition

A transitive model is a model $(M, \in)$ such that M is transitive, i.e. $\forall x \in M : x \subseteq M$.

Theorem (Löwenheim-Skolem, Mostowski)

Assume there is a model (M, E) of ZFC. Then there is a countable transitive model (ctm) M' of ZFC.

Lemma (Rasiowa-Sikorski)

Let M be a ctm of ZFC, $\mathbb{P}$ a forcing poset. Then there exists an M-generic filter $G \subseteq \mathbb{P}$.

Lemma (Rasiowa-Sikorski)

Let M be a ctm of ZFC, $\mathbb{P}$ a forcing poset. Then there exists an M-generic filter $G \subseteq \mathbb{P}$.

Proof: Let $\{D \text{ dense} \mid D \in M\} =: \{D_1, D_2, \dots\}$. Choose any $p_1 \in D_1$. D_2 is dense, so $\exists p_2 \in D_2 : p_2 \leq p_1$. D_3 is dense, so $\exists p_3 \in D_3 : p_3 \leq p_2$. This way, we choose $p_1 \geq p_2 \geq \dots$ with $p_i \in D_i$.
Set $G := \bigcup_{i \in \mathbb{N}} \{q \in \mathbb{P} : q \geq p_i\}$. This is a filter, and by construction it is M-generic since $p_i \in G \cap D_i$.

Names

Fix a ctm M of ZFC and a forcing poset $\mathbb{P} \in M$, $G \subseteq P$ a filter. We will construct $M[G]$ by defining names in M which will identify the objects in $M[G]$.

Definition

Define recursively:

- $\mathrm{Name}_0 := \emptyset$
- $\mathrm{Name}_{\alpha+1} := \mathcal{P}(\mathrm{Name}_\alpha \times \mathbb{P})$
- $\mathrm{Name}_\gamma := \bigcup_{\alpha<\gamma} \mathrm{Name}_\alpha$ for limit ordinals γ.

Set $\mathrm{Name} := \bigcup_{\alpha \in \mathrm{Ord}} \mathrm{Name}_\alpha$. Any $\sigma \in \mathrm{Name}$ is a $\mathbb{P}$-name.

Think of names as „sets with tags“. Just as sets contain other sets, names contain other names, but tagged with „labels“ from $\mathbb{P}$.
Note that $\mathrm{Name} \subseteq M$, so these names exist in M.

Defining $M[G]$

Definition

Let σ be a $\mathbb{P}$-name, let $G \subseteq \mathbb{P}$ be a filter. Recursively define

$$\sigma^G := \left\{ \tau^G \mid \exists p \in G : \langle \tau, p \rangle \in \sigma \right\},$$

the interpretation of σ. Now define $M[G] = \left\{ \sigma^G \mid \sigma \in \text{Name} \right\}$.

Example

To interpret a name, we „filter“ its elements through G:
Take $\mathbb{P} = \{0, 1\}$, $G = \{1\}$, $\sigma = \{\langle a, 0\rangle, \langle b, 1\rangle, \langle c, 1\rangle, \langle d, 0\rangle\} \in \text{Name}$.
Then $\sigma^G = \left\{ b^G, c^G \right\}$.

$M[G]$ makes sense

Proposition

$M \subseteq M[G]$ and $G \in M[G]$.

Proof: For any $x \in M$, recursively define $\check{x} := \{\langle \check{y}, 1 \rangle \mid y \in x\} \in$ Name.
Then (again by recursion), $\check{x}^G = \left\{\check{y}^G \mid y \in x\right\} = \{y \mid y \in x\} = x$.
For G, define $\Gamma := \{\langle \check{p}, p \rangle \mid p \in \mathbb{P}\} \in$ Name. Then
$\Gamma^G = \left\{\check{p}^G \mid p \in G\right\} = \{p \mid p \in G\} = G$.

Proposition

Let N be a transitive model with $N \models$ ZF, $M \subseteq N$ and $G \in N$. Then $M[G] \subseteq N$.

Proof: Since $N \models$ ZF, N contains all $\mathbb{P}$-names. Since $G \in N$, the definition of σ^G implies $\sigma^G \in N$ for any name σ. So $M[G] \subseteq N$.

The Forcing Relation

Definition

Let $p \in \mathbb{P}$ and let φ be a sentence. Then p forces φ iff $M[G] \models \varphi$ for all M-generic filters $G \ni p$. We notate this $p \Vdash \varphi$.

Truth Lemma

Let φ be a sentence, $p \in \mathbb{P}$ and $G \subseteq \mathbb{P}$ an M-generic filter. Then

$$M[G] \models \varphi \iff \exists p \in G : p \Vdash \varphi.$$

Definability Lemma

Let φ be a sentence and $p \in \mathbb{P}$. Roughly speaking, the statement $p \Vdash \varphi$ can actually be formulated *from* M. In particular, sets like $\{p \in \mathbb{P} \mid p \Vdash \varphi\}$ are actually in M.

$M[G] \models \mathrm{ZFC}$

Theorem

Let $G \subseteq \mathbb{P}$ be a generic filter. Then $(M[G], \in) \models \mathrm{ZFC}$.

(Part of the) Proof:

EmptySet $\emptyset = \emptyset^G \in M[G]$.

Extensionality Any transitive model satisfies Extensionality.

Pairing Take $\sigma^G, \tau^G \in M[G]$ and set $\rho := \{\langle\sigma, 1\rangle, \langle\tau, 1\rangle\} \in \mathrm{Name}$. Then $\left\{\sigma^G, \tau^G\right\} = \rho^G \in M[G]$.

Union Take $\sigma^G \in M[G]$ and set $\tau := \bigcup \mathrm{dom}(\sigma)$. For any $x \in \sigma^G$, we have $x = \rho^G$ for some $\rho \in \mathrm{dom}(\sigma)$. Now $\rho \subseteq \tau$, so $x = \rho_G \subseteq \tau_G$. Thus $\bigcup \sigma^G \subseteq \tau^G$.

Comprehension: For $\sigma_G \in M[G]$, $S := \{x \in \sigma_G \mid \varphi(x)\}$ is described by

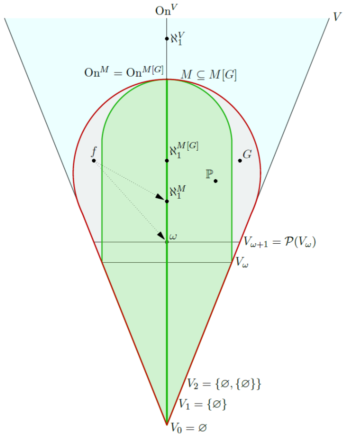
$$\tau = \{\langle\vartheta, p\rangle \mid \vartheta \in \mathrm{dom}\,\sigma, p \in \mathbb{P}, p \Vdash (\vartheta \in \sigma \wedge \varphi(\vartheta))\}.$$

$\tau \in \mathrm{Name}$ by Definability, and $\tau_G = S$ by Truth.

Breaking CH

We will use forcing to construct a model of ZFC + ¬CH.

When talking about cardinals, we have to be careful: $M[G]$ could have different cardinals than M.



Preserving cardinals

Definition

Let $\mathbb{P}$ be a poset. $X \subseteq \mathbb{P}$ is an antichain if $\forall a, b \in X : a \perp b$.
$\mathbb{P}$ has the countable chain condition if all antichains in $\mathbb{P}$ are countable.
We often abbreviate this as „$\mathbb{P}$ is ccc“.

Lemma

If J is countable, $\mathrm{Fn}(I, J)$ is ccc.

Theorem

Let $\mathbb{P}, \beta \in M$, $G \subseteq \mathbb{P}$ an M-generic filter and $M \models (\mathbb{P}$ is ccc$)$. Then
$M \models (\beta$ is a cardinal$) \Rightarrow M[G] \models (\beta$ is a cardinal$)$.
In particular, $\aleph_2^M = \aleph_2^{M[G]}$.

Breaking CH

Theorem

There is a model of ZFC $+ \neg$CH.

Proof: Let M be a ctm of ZFC and take $\mathbb{P} := \mathrm{Fn}(\aleph_2^M \times \omega, 2)$. Take $G \subseteq \mathbb{P}$ M-generic, so $f_G := \bigcup G \in M[G]$ is a function $f_G : \aleph_2^M \times \omega \overset{\text{onto}}{\longrightarrow} 2$.
For any $\alpha < \aleph_2^M$, define $h_\alpha : \omega \to 2, n \mapsto f_G(\alpha, n)$. Then $h_\alpha \in M[G]$ since $f_G \in M[G]$. If all the h_α are different, then we have built $\aleph_2^M$ many elements of 2^ω.
For any $\alpha < \beta < \aleph_2^M$, consider the set

$$E_{\alpha\beta} := \{p \in \mathbb{P} \mid \exists n[(\alpha, n), (\beta, n) \in \mathrm{dom}(p) \wedge p(\alpha, n) \neq p(\beta, n)]\}.$$

This is dense, so $G \cap E_{\alpha\beta} \neq \emptyset$ and $h_\alpha \neq h_\beta$.
Thus, we have $|(2^\omega)|^{M[G]} \geq \aleph_2^M = \aleph_2^{M[G]} > \aleph_1^{M[G]}$. This means $M[G] \models \neg$CH.

References I

[1] Kurt Gödel.
Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I.
Monatsh. f. Mathematik und Physik, 38-38(1):173–198, December 1931.

[2] Georg Cantor.
Ueber eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen.
Journal für die reine und angewandte Mathematik, 1874(77):258 – 262, 1847.

[3] P. J. Cohen.
THE INDEPENDENCE OF THE CONTINUUM HYPOTHESIS.
Proceedings of the National Academy of Sciences, 50(6):1143–1148, December 1963.

References II

[4] P. J. Cohen.
THE INDEPENDENCE OF THE CONTINUUM HYPOTHESIS, II.
Proceedings of the National Academy of Sciences, 51(1):105–110, January 1964.

[5] H. G. Dales and W. H. Woodin.
An introduction to independence for analysts.
Number 115 in London Mathematical Society lecture note series.
Cambridge University Press, Cambridge ; New York, 1987.

[6] In der Schweiz leben aktuell 810'000 Millionäre.
20 Minuten, October 2019.

[7] In der Schweiz gibt es 389 200 Millionäre.
Neue Zürcher Zeitung, June 2018.

References III

[8] Kurt Gödel.
The Consistency of the Axiom of Choice and of the Generalized Continuum-Hypothesis.
Proceedings of the National Academy of Sciences, 24(12):556–557, December 1938.

[9] Kenneth Kunen.
Set theory.
Number 34 in Studies in logic. College Publ, London, rev. ed edition, 2013.
OCLC: 915461876.

[10] Evan Chen.
An Infinitely Large Napkin.
self-published.