Contents

1 philosophical underpinnings

Through millions of years of evolution, we carbon sack computers have been tuned to take shortcuts. Even in the study of mathematics, these shortcuts are necessary: no one would teach an infant to count by formally proving $2 + 2 = 4$. But with these shortcuts leave us susceptible to logical fallacies.

To avoid these, we could start with assertions and then work toward a conclusion by requiring each new claim we make must logically follow from what we have already established, but English is too ambiguous and irregular. Consider the sentence

> Every mouse fears some cat.

Does this mean there is one terribly frightening cat that every single mouse fears? Or does it mean for each mouse there is a corresponding scary cat? [Wik15e]

The solution? A deductive system. One with a well-defined language for clear expression and well-defined rules for clear argumentation. It should be straight-forward enough that proofs can be checked by a computer, so we can claim absolute, or at least unambiguous, truth. To be useful, a deductive system must be expressive enough that we can work out all of mathematics. There is no right balance of these two concerns; each deductive systems balance them differently. They are not at odds with each other, although they seem to describe distinctive worlds.

I will be dodging the question 'is mathematics absolutely true?' In my eyes, a satisfying answer to this question must come from a mathematical analysis. This question is rather resilient to mathematical analysis, thanks to the ambiguity of natural language, the philosophical pitfalls absolutes bring, and even limitations on the mathematical end. Instead, we will pose a series of mathematical questions that approximate 'is mathematics absolutely true?', particularly, 'can this argument be algorithmically checked?' and 'are the valid arguments sensible?'

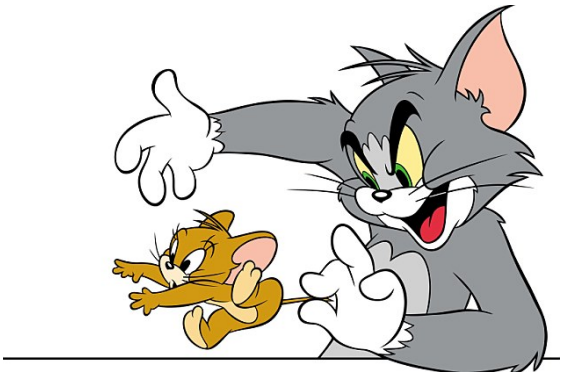


Figure 1.1: A scary cat

If we can algorithmically check arguments, we can approach a system of thought immune to subjectivity. This is not to say it is absolutely correct: if we're wrong, then we'll all be wrong together. We will elaborate on what sensible means as we go, but a 'sensible' argument should be free from contradictions, and should either agree with our intuition, or be able to show us the error in our ways.

How is this done? We will build a model of logical reasoning. With this scaffolding, we will build a model of mathematics. By studying these models, we glean some information about truth in mathematics.

We'll need logic to reason about our model. This circular reasoning can't be helped. It does pose a philosophical problem—we may very well be in the matrix, in which case everything we know is a lie, so our mathematical model could be dead wrong. I will assume without proof that we are not in the matrix. I will assume without proof that logic-checking computers do not lie. I will assume without proof that this circular reasoning is innocent.

2 boolean logic

The simplest interesting model of logic we will discuss. There are two possible values, true and false. When it is not ambiguous, we will abbreviate these as 0 and 1. Letters are variables. There are three operators we start with: and ($\wedge$), or ($\vee$), and not ($\neg$).

Definition 2.0.1 (and $\wedge$) $x \wedge y$ is true exactly when x and y are both true. This is also called conjunction.

$\wedge$	0	1
0	0	0
1	0	1

Definition 2.0.2 (or $\vee$) $x \vee y$ is true exactly when either x or y or both are true. This is also called disjunction.

$\vee$	0	1
0	0	1
1	1	1

Definition 2.0.3 (not $\neg$) Negation flips 0 and 1:

x	$\neg x$
0	1
1	0

Theorem 2.0.4 (De Morgan's law)

$$\neg(x \wedge y) = (\neg x) \vee (\neg y) \tag{2.1}$$
$$\neg(x \vee y) = (\neg x) \wedge (\neg y) \tag{2.2}$$

(see also [Wik15b])

Proof. First show eq. (2.1) by checking truth tables:

x	y	$x \wedge y$	$\neg(x \wedge y)$	$\neg x$	$\neg y$	$(\neg x) \vee (\neg y)$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

Then negate both sides of eq. (2.1), giving

$$x \wedge y = \neg(\neg x \vee \neg y)$$

Make the substitution $\bar{x} = \neg x$ and $\bar{y} = \neg y$:

$$(\neg\bar{x}) \wedge (\neg\bar{y}) = \neg(\bar{x} \vee \neg\bar{y})$$

or, equivalently, eq. (2.2). □

2.1 the conditional

We would like to model causality. Causality is vital in logical reasoning. But defining causality is a black hole ready to swallow up even the cleverest of thinkers. Instead we'll define the operator implies, a.k.a. the conditional, denoted $\rightarrow$, a stripped-down notion of causality.

Definition 2.1.1 (implies $\rightarrow$) $x \rightarrow y$ is true for all inputs except $1 \rightarrow 0$.

$\rightarrow$	0	1
0	1	1
1	0	1

This definition of captures the idea y must follow if x is true. But it allows for the possibility that y may occur even when x is false. For example, if x means 'that's a cat', and y means 'that's a mammal', $x \rightarrow y$ means 'that's a cat, hence it's a mammal', with the unspoken caveat that dogs are not cats ($x = 0$), but they are mammals ($y = 1$).

We defined the conditional through a truth table; however, our definition of boolean logic does not mention truth tables. We ought to give a definition of $\rightarrow$ using $\wedge$, $\vee$, and $\neg$:

Theorem 2.1.2 $x \rightarrow y$ is equivalent to $y \vee (\neg x)$

Proof. Both expressions are false only when $x = 1$ and $y = 0$. □

Definition 2.1.3 (logical equivalence $\leftrightarrow$) $x \leftrightarrow y$ exactly when $x = y$.

Likewise, we can define this in terms of $\wedge$, $\vee$, and $\neg$:

Theorem 2.1.4 $x \leftrightarrow y$ is equivalent to $(x \wedge y) \vee (\neg x \wedge \neg y)$.

2.2 tables to expressions

We have just translated two truth-tables into expressions consisting only of $\wedge$, $\vee$, and $\neg$. You might wonder if we can always do this. We can.

Theorem 2.2.1 (completeness) Every truth table has a corresponding boolean expression.

Table 2.1: some truthtable

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Proof. It's best to start with an example. Consider table 2.1 We want an expression that is true exactly when (x_1, x_2, x_3) is $(0, 0, 1)$ or $(1, 0, 0)$ or $(1, 1, 0)$. A straightforward way to do this is to or together a statement that is true only on the input $(0, 0, 1)$, a statement true only on $(1, 0, 0)$, and a statement that is true only on $(1, 1, 0)$.

Consider $(x_1, x_2, x_3) = (0, 0, 1)$. To find an expression that is true for this input and false for all others, we can simply assert $x_1 = 0$ and $x_2 = 0$ and $x_3 = 1$, *i.e.*

$$\neg x_1 \wedge \neg x_2 \wedge x_3$$

By the same argument, we can find the remaining expressions:

$$\begin{array}{ll} (x_1, x_2, x_3) = (0, 0, 1) & \neg x_1 \wedge \neg x_2 \wedge x_3 \\ (x_1, x_2, x_3) = (1, 0, 0) & x_1 \wedge \neg x_2 \wedge \neg x_3 \\ (x_1, x_2, x_3) = (1, 1, 0) & x_1 \wedge x_2 \wedge \neg x_3 \end{array}$$

Hence table 2.1 has expression

$$(\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3)$$

To prove the theorem, we just need to generalize the work we've done. Suppose we are given a truth table for the function $f(x_1, \ldots, x_n)$. Mark off the rows in the truth table where $f(x_1, \ldots, x_n) = 1$. For each such row, we construct the expression that asserts the input matches. If the current row is for the input

$$(x_1, \ldots, x_n) = (\alpha_1, \ldots, \alpha_n)$$

then the expression is

$$\begin{pmatrix} x_1 & \text{if } \alpha_1 = 1 \\ \neg x_1 & \text{if } \alpha_1 = 0 \end{pmatrix} \wedge \cdots \wedge \begin{pmatrix} x_n & \text{if } \alpha_n = 1 \\ \neg x_n & \text{if } \alpha_n = 0 \end{pmatrix}$$

Abbreviate this as $(x_1 = \alpha_1) \wedge \cdots \wedge (x_n = \alpha_n)$. This is just a notational convenience; the final answer will not actually contain $=$ or refer to the α_i.

Or over each of the above expressions:

$$f(x_1, \ldots, x_n) = \bigvee_{\alpha_1, \ldots, \alpha_n : f(\alpha_1, \ldots, \alpha_n) = 1} (x_1 = \alpha_1) \wedge \cdots \wedge (x_n = \alpha_n)$$

giving the desired expression. □

This tells us that boolean logic is big enough to express any truth table. An interesting implication is that general purpose computers can be constructed!

2.3 absolute truth?

Boolean logic is simple enough that we can talk about absolute truth without making a mess. Trusting boolean algebra is about as reasonable as trusting a calculator for integer arithmetic. A boolean expression's truth value can be computed directly from the inputs. Since each input can be either true or false, there are only finitely many possible inputs. Everything you need to know is contained in the expression's truth table. These computations can be carried out unambiguously by a machine in finite time, so things are looking pretty good.

A statement and its negation cannot be true simultaneously, *i.e.*

$$p \wedge \neg p = 0$$

for any expression p. No matter what p is, it must evaluate to either 1 or 0. Suppose $p = 1$. Then $\neg p = 0$. So $p \wedge \neg p = 1 \wedge 0 = 0$. Likewise, if $p = 0$, we get $0 \wedge 1 = 0$.

3 predicate logic

Boolean logic is beautiful, but it is not expressive enough to make deductions like 'Socrates is a man. All men are mortal. Therefore, Socrates is mortal.'

Nineteenth century mathematics was in crisis. For thousands of years, mathematics had remained essentially unchanged: the gold standard was proof by Euclidean geometry. Algebra, arabic numerals, zero were tools to expedite geometric reasoning. Even new results in number theory were assumed to be, at heart, geometric truths. But by the 1800s, it was clear this worldview was no longer sustainable. Mathematics had grown too abstract.

Calculus, the most revolutionary discovery this side of the dark ages, stood with embarrassingly poor theoretical footing. Newton and Leibniz through Euler and Cauchy relied on infinitesimals, but could not justify their use *a priori*, certainly not by Euclidean geometry. To make matters worse, if you were not careful, an argument that seemed kosher could result in nonsense. Fourier's work was downright scandalous. He was able to solve the heat equation, a problem unsolved for all but the most trivial cases. Experiments verified his results, but conservative mathematicians refused to accept his method.

Abel, and later Galois, proved that degree 5 equations have no general solution that can be written in terms of the basic arithmetic operations and radicals. In particular, the crux of Galois's proof were abstract systems with no clear base in Euclidean geometry.

Even Euclidean geometry was proving to be less than the paragon of flawless logic it once seemed. Problems in Euclidean geometry went unsolved for millenia, like can you trisect an angle with a compass and straightedge went unsolved for a few millennia. But these were quickly solved using Galois's tools[Wik15a]. Euclid's parallel axiom was thought to be provable from his other axioms for thousands of years, but it was shown in the mid 19th century that was impossible. Euclid's remaining axioms are satisfied by spherical and hyperbolic geometry. In each, Euclid's parallel postulate does not hold.

In the nineteenth century, mathematics outgrew its ontology. The situation was so disorienting, Dodgson wrote a veiled satire ridiculing the absurdity of this new mathematics. Dodgson is better known as Lewis Carol. This satire is called *Alice in Wonderland*.[Ang15]

Gottlob Frege laid the foundations for mathematics' new ontology. Whereas George Boole's logic was viewed more as a useful trick that cleaned up some ambiguities for the pedants, Frege developed a logic capable of housing all of the new mathematical objects. His work went relatively unnoticed by his contemporaries, but it revolutionized mathematics and philosophy.

3.1 what is predicate logic?

First order predicate logic is the modern descendant of Frege's logic. It is more expressive than boolean logic, making it both critical to our modern understanding of mathematics, and complicated enough that we can't declare it absolutely true.

Predicate logic makes use of the same operations and conventions of boolean logic ($\wedge$, $\vee$,$\neg$,$\rightarrow$,$\leftrightarrow$ and variables), but adds constant symbols, function symbols, predicate symbols, quantifiers, and a special equality predicate.

These additions allow us to talk in generalities about entities that live in some universe, for example the natural numbers.

Definition 3.1.1 (constant symbols) Constant symbols name specific entities in the universe.

Example 3.1.2 (constant symbols) 0, 1, 30, 10 are constant symbols referring to natural numbers.

Definition 3.1.3 Function symbols name functions that take in entities and output an entity.

The arity of a function is the number of arguments it takes, *e.g.* $+$ has arity 2. Functions do not reside in the proverbial universe. If we are working in a universe of natural numbers, we will want to refer to $+$. But $+$ is not a number. It belongs in a separate bin.

Example 3.1.4 $+, \times$ are functions of natural numbers.

Definition 3.1.5 (predicate symbols) Predicate symbols name predicts, which take in entities and output true or false. Like functions, predicates have arity and exist outside of the universe. But predicates are distinct from functions. Predicates output truth values, but functions output elements of the universe (*e.g.* natural numbers). If add two numbers, you can multiply the result by 2: $(1 + 3) \times 2$. You cannot, however, say $(1 < 3) + 5$.

Example 3.1.6 $<, \geqslant, =$ are predicates of natural numbers

Definition 3.1.7 (quantifier) Quantifiers allow us to talk about general elements in the universe. There are two quantifiers: $\forall$, read as 'for every', and $\exists$, read as 'there exists'.

Intuitively, $\forall x.\phi(x)$ means $\phi(x)$ is true, no matter what x is in the universe, and $\exists x \phi(x)$ means somewhere in the universe, there is an x that satisfies ϕ. We will make this exact through inference rules later.

If we refer to Socrates by the constant symbol s, we can state the syllogism 'Socrates is a man. All men are mortal. Hence, Socrates is mortal' as follows:

$$\texttt{man?}(s) \wedge \forall x \big(\texttt{man?}(x) \rightarrow \texttt{mortal?}(x)\big) \rightarrow \texttt{mortal?}(s)$$

Recall the statement

> Every mouse fears some cat

We can now state this unambiguously as

$$\forall m \big(\texttt{mouse?}(m) \rightarrow \exists c(\texttt{cat?}(c) \wedge \texttt{fears?}(m, c))\big)$$

i.e. 'for every mouse, we can find a cat which that specific mouse fears.'

$$\exists c \big(\texttt{cat?}(c) \wedge \forall m(\texttt{mouse?}(m)\texttt{fears?}(m, c)\big)$$

i.e. 'there is one particularly frightening cat all mice fear'.

Definition 3.1.8 (equality) Equality is a predicate that always satisfies the following axioms

1. Reflexivity: $\forall x(x = x)$
2. Substitution: equal elements are interchangeable

   for all functions f: $\forall x \forall y(x = y \to f(x) = f(y))$[1]

   for predicates ϕ: $\forall x \forall y \Big(x = y \to \big(\phi(x) \leftrightarrow \phi(y)\big)\Big)$

3.2 peano arithmetic

I promised this would be sufficient to house modern mathematics. I will show you how the natural numbers can be defined using Peano's axioms [Wik15d].

Definition 3.2.1 (Peano arithmetic) There is a constant called 0 and a function of one argument called succ, essentially $\_ + 1$. The Peano axioms are as follows:

1. Nothing comes before zero:
$$\forall x.0 \neq \mathrm{succ}(x)$$
2. Two naturals are equal if their successors are equal:
$$\forall x \forall y \big(\mathrm{succ}(x) = \mathrm{succ}(y) \to x = y\big)$$
3. Induction: if ϕ is a predicate,
$$\phi(0) \wedge \forall x \big(\phi(x) \to \phi(\mathrm{succ}(x))\big) \to \forall y.\phi(y)$$
   i.e., if $\phi(0)$ and $\phi(s)$ implies $\phi(s + 1)$, then ϕ must be true for all natural numbers.

Definition 3.2.2 (plus) We can define $+$, a function of two inputs, by recursion:

$$\forall x(x + 0 = x)$$
$$\forall x \forall y \big(x + \mathrm{succ}(y) = \mathrm{succ}(x + y)\big)$$

3.3 deduction

In boolean algebra, when determining the truth of a statement, the worst case scenario will require writing out a large truth table. Not so for predicate logic. Quantifiers range over everything in some possibly infinite universe. Predicates abstract away calculations to something behind the scenes. Without a way to explicitly list everything in the universe, the logician must indicate its content, as well as the behavior of some predicates, with axioms.

[1] Quantifiers range over the universe. But functions don't live in the universe. So we can't write something like $\forall f \forall x \forall y(x = y \to f(x) = f(y))$. The solution is to treat this condition as a template, or *axiom schema*, and copy it over for each function.

Some axioms, like $\forall x.P(x)$ and $\exists x.\neg P(x)$ are contradictory, hence nonsensical. One would hope this is just a case of 'ask a bad question; get a bad answer'. We would hope that the laws of deduction, which govern what you can actually do with the axioms you choose, are ok.

For $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$, deduction works the same as it did for boolean logic:

$x \wedge y$ is true if and only if (iff) x is true and y is true

$x \vee y$ is true iff x is true or y is true

$\neg x$ is true iff x is false

$x \rightarrow y$ is true unless $x = 1$ and $y = 0$

$x \leftrightarrow y$ is true iff x has the same truth value as y

Universal Introduction—if we know $\phi(\alpha)$, we can conclude $\forall\alpha.\phi(\alpha)$ so long as α is unused elsewhere.

Universal Elimination—if we know $\forall\alpha.\phi(\alpha)$ then we can conclude $\phi(\beta)$.

Existential Introduction—if we know $\phi(\beta)$ then we can conclude $\exists\alpha\phi(\alpha)$ so long as α is previously unused.

Existential Elimination—if we know $\exists.\alpha\phi(\alpha)$, we can say $\phi(\beta)$ so long as β is previously unused.

Applications of some rules may require renaming variables. This is no problem as long as the meaning of the statement is not changed (*i.e.* two things that used to have different names cannot have the same name).

3.4 some proofs

We are now prepared to prove things about Peano arithmetic:

Theorem 3.4.1 ($+$ is associative) The statement

$$\forall x\forall y\forall z.(x + y) + z = x + (y + z)$$

is deducible from Peano arithmetic and the definition of plus.

Proof. Short version—this is a proof by induction. First, we prove the base case:

$$\forall a\forall b.(a + b) + 0 = a + (b + 0) \tag{3.1}$$

Equivalently, $\phi(0)$ where

$$\phi(x) = \forall a\forall b.(a + b) + x = a + (b + x)$$

Noting that $y + 0 = y$, (see the definition of plus), we see eq. (3.1) is, in fact, true.

Now we prove the inductive step:

$$\forall x\big(\phi(x) \rightarrow \phi(\mathsf{succ}(x))\big) \tag{3.2}$$

Pick a, b, and c. Assume $(a + b) + c = a + (b + c)$, which we abbreviate as $a + b + c$. Now consider $(a + b) + \mathsf{succ}(c)$. By definition of plus, we see

$$(a + b) + \mathsf{succ}(c) = \mathsf{succ}(a + b + c)$$

Similarly,

$$a + (b + \mathsf{succ}(c)) = a + \mathsf{succ}(b + c) = \mathsf{succ}(a + b + c)$$

hence $(a + b) + \mathsf{succ}(c) = a + (b + \mathsf{succ}(c))$. This proves the inductive step, eq. (3.2).

To finish the proof, use the induction axiom. □

The above proof does not justify each step, but gives enough information to show how deduction works. This is the norm for mathematical proofs. Actually, this proof is boring when you are studying the mathematics of the natural numbers: it is not hard to convince someone addition is associative.

But since we want to understand the very fabric of reason itself, it must be possible to write out this proof in such painstaking detail that a computer, or even the most pedantic of logic professors, can follow it. Such a proof may look like the following:

Proof. Full gory details—First establish the base case, eq. (3.1) Consider the statement $(a+b)+0$. By definition 3.2.2, we know $\forall x.x+0 = x$. By universal elimination, deduce $(a+b)+0 = a+b$. Now consider $a + (b + 0)$. By universal elimination, deduce $b + 0 = b$. By substitution, deduce $a + (b + 0) = a + b$. Then, by transitivity, we know $(a + b) + 0 = a + (b + 0)$. As a and b are totally arbitrary free variables, two universal introductions establish eq. (3.1).

Now the inductive step, eq. (3.2) Assume

$$(a + b) + c = a + (b + c) = a + b + c \tag{3.3}$$

Consider the statement $(a + b) + \mathsf{succ}(c)$. From definition 3.2.2, we know

$$\forall x \forall y.x + \mathsf{succ}(y) = \mathsf{succ}(x + y)$$

An analogous quantifier elimination gives $(a + b) + \mathsf{succ}(c) = \mathsf{succ}(a + b + c)$. Another quantifier elimination gives $a+(b+\mathsf{succ}(c)) = a+\mathsf{succ}(b+c)$. A final quantifier elimination gives $a+\mathsf{succ}(b+c) = \mathsf{succ}(a+b+c)$. Transitivity gives $(a+b)+\mathsf{succ}(c) = a+(b+\mathsf{succ}(c))$. We can stop assuming eq. (3.3), rephrasing our work so far as

$$(a + b) + c = a + (b + c) \to (a + b) + \mathsf{succ}(c) = a + (b + \mathsf{succ}(c))$$

Now a, b, and c are arbitrary, so we can use a triple quantifier introduction to prove eq. (3.2).

As we have shown eqs. (3.1) and (3.2) we can deduce

$$\phi(0) \wedge \forall x\big(\phi(x) \to \phi(\mathsf{succ}(x))\big) \tag{3.4}$$

By the induction axiom,

$$\phi(0) \wedge \forall x\big(\phi(x) \to \phi(\mathsf{succ}(x))\big) \to \forall x \phi(x)$$

Then using boolean logic (*modus ponens*), conclude $\forall z \phi(z)$. Hence, $+$ is associative. This proves the theorem. □

Ironically, justifying each step results in a proof that is harder for a human to understand.

3.5 the death of reason

Once mathematicians started actually reading Frege, it was not long until they would dream the impossible dream. Hilbert and his entourage longed for a world in which mathematics had been effectively solved, the right axioms were chosen, and a machine would be built that would write out every true theorem until the end of time. All mathematicians would then be free to sip martinis poolside as an endless tickertape listing all true things would scroll by. [Wik15c]

The mathematicians would have to really read this carefully every now and then to answer a physicist's question. But they discovered by speaking in gratuitous generalities and shouting 'the proof is trivial' rather frequently, they could make a pesky physicist disappear, ensuring a veritable utopia (see http://www.smbc-comics.com/index.php?db=comics&id=2675#comic). Thus French Formalism was born.

But, one fateful night in 1931, dear reader, a young Kurt Gödel dealt a fatal blow to the Hilbertian dream of mathematical rapture. He was merely engaging in the logician's favorite pass-time: making things mercilessly meta. As many a logician and patron of webcomics know, making things meta may make a mess, and a major mess it made moreover. To his merit, this metamethematical misfortune marks the makings of a modern mathematical maturity, one more meaningful than a mere mirage marred by the multitude of mathematical models and their unmarried meandering truths. Any system of mathematics sufficiently sophisticated to serve as semantics for something like Peano's arithmetic suffers from a malady said to be incompleteness. See, m'lady, such a malady means more than several true-seeming statements may lay beyond reach of the most surefire machines of Hilbert's dreams.

3.5.1 berry's paradox

There are only so many numbers you can name in under eleven words, finitely many in fact. So consider the smallest positive integer not nameable in under eleven words. Surely it exists; every nonempty set of naturals has a least number (exercise for the reader!). When considering how many words it takes to name this number, 10 is right out. Except, of course, I named it in 10 words: 'the(1) smallest(2) positive(3) integer(4) not(5) nameable(6) in(7) under(8) eleven(9) words(10)'.

3.5.2 incompleteness

This proof is due to George Boolos. Gödel's proof used the liar's paradox (this sentence is false), which leads to a longer proof.[Wik15f] In both cases, the genius of the proof lies in encoding these paradoxes into Peano arithmetic.

Definition 3.5.1 (Gödel numbering) A Gödel numbering is a lossless encoding of first order logical statements in the natural numbers. Many such encodings exist. For our purposes, any one will work.

Once we pick a Gödel numbering, Peano arithmetic becomes self-referential.

Definition 3.5.2 (names) A formula F names the number n iff $\forall x(F(x) \leftrightarrow x = n)$.

Now we define some predicates:

Definition 3.5.3 (nameln?) $\texttt{nameln?}(x, y)$ is true iff x can be named by a statement containing y symbols. We can define this purely in terms of arithmetic operations via our Gödel numbering.

Definition 3.5.4 (smaller?)

$$\texttt{smaller?}(x, y) \leftrightarrow \exists z.z < y \wedge \texttt{nameln?}(x, z)$$

i.e. $\texttt{smaller?}(x, y)$ iff x can be named by a statement with length less than y.

Definition 3.5.5 (nodef?)

$$\texttt{nodef?}(x, y) \leftrightarrow \neg\texttt{smaller?}(x, y) \wedge \forall a\big(a < x \rightarrow \texttt{smaller?}(a, y)\big)$$

i.e. $\texttt{nodef?}(x, y)$ iff x is the smallest number that cannot be named in y symbols.

Definition 3.5.6 (berry?)

$$\texttt{berry?}(x) \leftrightarrow \exists y.y = \texttt{succ}^{10}(0) \cdot \texttt{succ}^{k}(0) \wedge \texttt{nodef?}(x, y)$$

where $\cdot$ is multiplication, $\texttt{succ}^n$ abbreviates n applications of succ, and k is the length of $\texttt{nodef?}(x, y)$. This encodes Berry's paradox in Peano arithmetic.

Theorem 3.5.7 (Gödel's first incompleteness) There is some statement that cannot be proved true or false in Peano arithmetic.[2]

Proof. We will construct such a statement. Let N be the smallest number that cannot be named in fewer than $10k$ symbols. Define

$$\forall x\big(\texttt{berry?}(x) \leftrightarrow x = \texttt{succ}^{N}(0)\big) \tag{3.5}$$

As $\texttt{berry?}(x)$ places a minimality condition on x via the $\texttt{nodef?}(x, y)$ term, at most one element can satify $\texttt{berry?}(x)$. Thus, a proof of eq. (3.5)'s negation amounts to showing N does not satisfy berry?. Suppose such a proof exists and $\texttt{berry?}(N)$ is false. But N was chosen specifically to satisfy berry?, a contradiction.

A proof of eq. (3.5) would prove berry? names N in fewer than $10k$ symbols, a contradiction.□

[2] Assuming Peano arithmetic is consistent (free of contradictions).

4 set theory

While Frege was laying the groundwork for a new ontology of mathematics, Cantor proposed a controversial theory of infinite sets. Today, this theory is used to give us a big enough universe to do almost all of mathematics.

While investigating an unsolved problem in analysis, Cantor found a solution that required numbers beyond infinity. The mathematics of his time had no way to make sense of such large numbers. Captivated, Cantor turned his focus to making the infinite precise. Conventional wisdom said this was not possible. Cantor believed that, not only was this possible, but progress in mathematics required it.

To lay foundations on which he could build his theory the infinite, Cantor invented set theory. These sets were just collections of objects that were possibly infinite. Next, he looked for a way to compare the size of infinite objects. Once he accomplished this, he was able to show that some infinite sets were smaller than others. Initially, this idea was met with both derision and celebration. Gradually, mathematics came to see the necessity of Cantor's insights. Today, you can't get far in mathematics without running into sets.

4.1 naïve set theory

Definition 4.1.1 (naïve set) A set is an unordered collection of mathematical objects. A set may be infinite. Two sets are the same if they have the same elements, *e.g.* $\{1,2,3\} = \{2,1,3\} = \{3,2,1\}$ because the elements are the same and order doesn't matter.

Definition 4.1.2 (member) We say y is an element of the set X if X contains y. This is written $y \in X$.

Definition 4.1.3 (subset $\subseteq$) A set X is a subset of Y, written $X \subseteq Y$, if and only if (iff) every element of X is also an element of Y.

Example 4.1.4 The collection $\mathbb{N}$ is the set of all natural numbers. It is infinite. The set of even numbers E is a subset of $\mathbb{N}$, *i.e.* $E \subseteq \mathbb{N}$.

One may take unions ($\cup$) and intersections ($\cap$) of sets.

Now we would like to know how to compare the sizes of infinite sets.

Definition 4.1.5 Two sets X and Y are in a 1-to-1 correspondence if we can match each element of X with exactly one element of Y and have no elements in Y left over.

Example 4.1.6 The sets $\{1, 2, 3\}$ and $\{5, 6, 7\}$ are in a 1-to-1 correspondence, namely

$$\begin{aligned} 1 &\mapsto 5 \\ 2 &\mapsto 6 \\ 3 &\mapsto 7 \end{aligned}$$

There are other 1-to-1 correspondences between these sets.

Example 4.1.7 The set $\mathbb{N}$ (natural numbers) is in a 1-to-1 correspondence with E (even numbers).

$$\begin{aligned} 0 &\mapsto 0 \\ 1 &\mapsto 2 \\ 2 &\mapsto 4 \\ &\vdots \\ n &\mapsto 2n \\ &\vdots \end{aligned}$$

Definition 4.1.8 (size) Two sets have the same size iff there is a 1-to-1 correspondence between them.

So we can see there are as many even numbers as there are natural numbers. Likewise, there are as many even numbers as odd numbers.

Theorem 4.1.9 There set of natural numbers ($\mathbb{N}$) and integers ($\mathbb{Z}$) have the same size.

Proof.

$$\begin{array}{lccccccc} \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & \dots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{Z}: & 0 & 1 & -1 & 2 & -2 & \dots \end{array}$$

□

Theorem 4.1.10 The set $\mathbb{N}$ (natural numbers) has the same size as $\mathbb{N}^2$ (pairs of natural numbers).

Proof. Lay out $\mathbb{N}^2$ in the following grid:

$$\begin{array}{ccccccccccc} & & & & & (0,0) & & & & & \\ & & & & (0,1) & & (1,0) & & & & \\ & & & (0,2) & & (1,1) & & (2,0) & & & \\ & & (0,3) & & (1,2) & & (2,1) & & (3,0) & & \\ & (0,4) & & (1,3) & & (2,2) & & (3,1) & & (4,0) & \\ \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \end{array}$$

Reading off each row from the top gives the following 1-to-1 correspondence:

$$\begin{array}{lcccccc} \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & \dots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{N}^2: & (0,0) & (0,1) & (1,0) & (0,2) & (1,1) & \dots \end{array}$$

□

Theorem 4.1.11 The set $\mathbb{N}$ (natural numbers) is the same size as $\mathbb{Q}$ (rational numbers)

Proof. Lay out $\mathbb{Q}$ in the following grid, writing only the fractions that are in simplest form:

$$
\begin{array}{cccccccc}
0 & & & & & & & \\
\frac{-1}{1} & \frac{1}{1} & & & & & & \\
\frac{-1}{2} & \frac{1}{2} & & & & & & \\
\frac{-2}{3} & \frac{-1}{3} & \frac{1}{3} & \frac{2}{3} & & & & \\
\frac{-3}{4} & \frac{-1}{4} & \frac{1}{4} & \frac{3}{4} & & & & \\
\frac{-4}{5} & \frac{-3}{5} & \frac{-2}{5} & \frac{-1}{5} & \frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} \\
\vdots & & & & & & &
\end{array}
$$

Reading off from the top gives a 1-to-1 correspondence:

$$
\begin{array}{lccccccc}
\mathbb{N}: & 0 & 1 & 2 & 3 & 4 & \dots \\
 & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\
\mathbb{Q}: & 0 & -1/1 & 1/1 & -1/2 & 1/2 & \dots
\end{array}
$$

□

Definition 4.1.12 (countably infinite) If a set has the same size as the natural numbers, it is countably infinite.

Theorem 4.1.13 (uncountably infinite sets exist) The set $2^{\mathbb{N}}$ of infinite binary strings[1] is uncountable.

Proof. Suppose $2^{\mathbb{N}}$ is countably infinite. Then there is some 1-to-1 correspondence between $2^{\mathbb{N}}$ and $\mathbb{N}$. We can think of this as a numbered list of all the elements of $2^{\mathbb{N}}$. For argument's sake, lets say this list is

$$
\begin{array}{lcccccccc}
0 & \mapsto & 0 & 0 & 0 & 0 & 0 & \dots \\
1 & \mapsto & 1 & 0 & 0 & 0 & 0 & \dots \\
2 & \mapsto & 0 & 1 & 1 & 0 & 0 & \dots \\
3 & \mapsto & 0 & 0 & 1 & 0 & 1 & \dots \\
4 & \mapsto & 0 & 1 & 0 & 1 & 1 & \dots \\
\vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

[1] This notation is chosen because of the convention $2 = \{0, 1\}$. Then $2^{\mathbb{N}}$ is the set of infinite sequences of 1 or 0.

Now consider the diagonal entry, in this case

$$0, 0, 1, 0, 1 \ldots$$

Negating each term gives

$$x = 1, 1, 0, 1, 0 \ldots$$

As x is an infinite sequence of 0 and 1s, we know $x \in 2^{\mathbb{N}}$. We are assuming every element in $2^{\mathbb{N}}$ will show up eventually in our list; thus x must eventually show up. But x cannot be entry 0 because their 0-th terms differ. Likewise, x cannot be the entry 1 because their 1-th terms differ. In general, x cannot be element number M because the M-th terms will differ. So, in fact, x does not show up anywhere in our list, a contradiction.

I gave specific examples for clarity. But for any list of elements of $2^{\mathbb{N}}$, we can find an x by negating the diagonal. Then the argument that x cannot be the first, second, third,...M-th term still works, regardless of the specific values. There is no 1-to-1 correspondence between M and $2^{\mathbb{N}}$ because such a correspondence would lead to a contradiction. □

This is the first notable result of the chapter. When Cantor discovered this, it showed the world infinite sets could be understood mathematically, and infinite sets were more complicated than they appeared. You may wonder if there are sets strictly bigger than $2^{\mathbb{N}}$. There are. In fact, there are infinitely many.

4.2 russell's paradox

Cantor's results were initially met with skepticism. Mathematicians found his results so counter-intuitive that some suspected they were nonsense. Today you would be hard-pressed to find a mathematician who did not believe Cantor's results, but Cantor's work was free of error. In fact, philosopher-mathematician-politician Bertrand Russell found a glaring error in Cantor's work, known as Russell's paradox:

Consider the set

$$R = \{x : x \notin x\}$$

i.e. the set of sets that don't contain themselves. Russell asked, 'does R contain itself ($R \in R$)?' Suppose it does. By definition of R, all sets in R must not contain themselves. Then $R \notin R$, a contradiction. Suppose $R \notin R$. Then, as R does not contain itself, by definition of R, in fact $R \in R$, a contradiction.

Cantor was used to hearing grievances aired about his work, but this shocked Frege. It also demonstrated his attempt to build mathematics out of logic led to contradictions. Mathematicians persevered in their quest to formalize mathematics. Bertrand Russell, along with his mentor Alfred N. Whitehead, spent a decade trying to lay the logical foundations of mathematics in a way that avoided paradoxes like this. In particular, they were looking for a foundation that was *consistent*—free of contradictions—and *complete*—everything can be proved true or false.

To avoid Russel's paradox, they built their mathematical universe in layers. In each layer, definitions can only refer to things defined in the layers below. In this system, there is no way to define the set of all sets that contain themselves. They could not show this theory, which

they laid out in *Principia Mathematica*[2] was either consistent or complete.[3] *Principia* is so complicated it takes over 360 pages to prove $1 + 1 = 2$[Mat].

In practice, the layers in *Principia* are superfluous for normal mathematics. Usually we can get away with just providing axioms governing the definitions of sets. The right axioms will prevent the paradoxes Russell & Whitehead feared.

4.3 axiomatic set theory

In mathematics today, the conventional foundation is *Zermelo-Fraenkel Set theory with the Axiom of Choice* (ZFC). To prove a theorem, you show that it can be proved by the deduction laws for first order logic starting with the axioms of ZFC. Of course, this is rarely done in practice; such proofs would be incomprehensible to most people. We will not prove things from the axioms of ZFC. In fact, we will only explicitly use some of ZFC's axioms. But underneath our proofs is the assumption that the proof can be written out fully, starting with the axioms of ZFC, so that a proof-checking computer would accept it.

Define ZFC as a first-order theory with the constant symbol $\varnothing$, which is the empty set. There is a predicate symbol $\in$ for membership, *i.e.* $x \in y$ iff x is an element of y. The axioms are as follows:

1. Extensionality
   Two sets are the same if they have the same elements. In other words, everything you need to know about a set is determined by its elements.
   $$\forall x \forall y \big(\forall z (z \in x \leftrightarrow z \in y) \rightarrow (x = y)\big)$$

2. Regularity
   Every nonempty set is disjoint from at least one of its elements
   $$\forall x (x \neq \varnothing \rightarrow \exists y . y \in x \wedge y \cap x = \varnothing)$$
   This prevents sets from containing themselves.

3. Specification
   For any set X, we can find a subset containing exactly those elements of X that satisfy a predicate of our choosing. If we call this predicate ϕ, then
   $$\forall X \exists Y \forall z (z \in X \wedge \phi(z) \leftrightarrow z \in Y)$$
   Sets constructed with this axiom will often be written in set builder notation:
   $$\{x \in \mathbb{N} : \exists k \in \mathbb{N} \text{ such that } x = 2k\}$$
   is the set of even natural numbers.

[2] Named after Newton's book.
[3] Gödel would later show both goals were impossible.

4. Singletons
   For any x, there is a set which contains x.

   $$\forall x \exists Y . x \in Y$$

   This axiom is usually used with specification to get the set $\{x\}$. Such one-element sets are called singletons. We will not use this axiom explicitly, but we will always assume this can be done.

5. Union
   You can take unions, even if they're infinite. For any set of sets X, there is a set that accumulates the contents of every element of X. This may be written

   $$U = \bigcup X$$

   or, more frequently, by writing $X = \{X_i : i \in I\}$ where I is a set of indexes,

   $$U = \bigcup_{i \in I} X_i$$

   This definition allows for infinite unions, which are rather useful.

   The first order sentence is

   $$\forall X \exists U \forall Y \big(Y \in X \to \forall z (z \in Y \to z \in U) \big)$$

6. Replacement
   Suppose the predicate $\phi(x, y)$ encodes a function, *i.e.*

   $$\forall x \exists ! y \phi(x, y)$$

   where $\exists ! y$ means there is exactly one y with the required property. You can think of this as a shorthand for

   $$\forall x \exists y \forall z (\phi(x, z) \to z = y)$$

   The axiom of replacement states the image of a set X under the function encoded by ϕ is also a set. We can *replace* X with its image Y to get a set.

   $$\forall X \exists Y \forall x \forall y (x \in X \wedge \phi(x, y) \to y \in Y)$$

   We not will use this axiom explicitly.

7. Infinity
   The natural numbers exist. Specifically, we say $0 = \varnothing$. Also, let $\mathrm{succ}(x) = x \cup \{x\}$. Then

   $$\exists \mathbb{N} . \varnothing \in \mathbb{N} \wedge \forall n (n \in \mathbb{N} \to \mathrm{succ}(n) \in \mathbb{N})$$

   Once we have the natural numbers, we can create all the infinite sets we want, but without it we can only construct finite sets.

8. Powerset
   The powerset of X, denoted 2^X, is the set of subsets of X. This axioms guarantees that the powerset of set X is also a set.

$$\forall X \exists 2^X \forall z (z \subseteq X \leftrightarrow z \in 2^X)$$

9. Choice
   This is the most famous and controversial of the ZFC axioms. It says, for any set of nonempty sets, X, we can assume there exists a corresponding *choice function*. If we write X in index notation, $X = \{X_i : i \in I\}$, then a choice function is a function f such that $f(X_i) \in X_i$. In other words, we can assume there is a way to pick an element from each set in X. We defer the first-order sentence stating this axiom until we have talked about functions.

The work we did before can be formalized in this system:

Definition 4.3.1 (ordered pair)

$$(x, y) = \big\{\{x\}, \{x, y\}\big\}$$

This way, we can distinguish between

$$(x, y) = \big\{\{x\}, \{x, y\}\big\}$$

and

$$(y, x) = \big\{\{y\}, \{x, y\}\big\}$$

Definition 4.3.2 (ordered tuple) We define the ordered tuple

$$(x_0, \ldots, x_n) = \{(0, x_0), (1, x_1), \ldots, (n, x_n)\}$$

Definition 4.3.3 (cartesian product) Suppose X and Y are sets. Their cartesian product, denoted $X \times Y$, is the set of ordered pairs (x, y) where $x \in X$ and $y \in Y$.

Definition 4.3.4 (function) A function f from X to Y, or

$$f : X \to Y$$

is a subset of $X \times Y$ where each x in X is paired with one and only one y in Y, *i.e.*

$$\forall x \big(x \in X \to \exists! y . y \in Y \wedge (x, y) \in f\big)$$

The set of functions from X to Y is denoted by Y^X.

Definition 4.3.5 (1-to-1 correspondence) A 1-to-1 correspondence between X and Y is a function $f : X \to Y$ with the property that each $y \in Y$ is the image of exactly one $x \in X$, *i.e.*

$$\forall y (y \in Y \to \exists! x . f(x) = y)$$

4.4 to infinity and beyond

At the opening of this chapter, you were promised we'd count past infinity. But first, a quick detour through order theory:

Definition 4.4.1 (well-ordered) A set X with an order $\leqslant$ is well-ordered iff every nonempty subset of X has a least element.

Example 4.4.2 The set $\mathbb{N}$ with order $\leqslant$ is well-ordered. To see this, note that a natural number is a set of all the natural numbers before it.

$$\begin{aligned} 0 &= \{\} \\ 1 &= \{0\} \\ 2 &= \{0, 1\} \\ 3 &= \{0, 1, 2\} \\ &\vdots \end{aligned}$$

If X is a nonempty subset of $\mathbb{N}$,

$$n = \bigcap X$$

gives the set of all numbers smaller than everything in X, *i.e.* n is the least element of X.

Example 4.4.3 The set $\mathbb{Z}$ (integers) with order $\leqslant$ is not well-ordered. The easiest way to show this is to consider $\mathbb{Z}$, a subset of $\mathbb{Z}$. There is no smallest integer, so this subset has no least element.

Each natural number is finite. But we can define an infinite number, one that is greater than all natural numbers.

Definition 4.4.4 (ω) Define

$$\omega = \mathbb{N}$$

Define $x < y$ if $x \in y$. Then ω is greater than every natural number.

This new number ω cannot be a successor of a natural number, as it is not a natural number. But we can say

$$\mathsf{succ}(\omega) = \omega \cup \{\omega\} = \mathbb{N} \cup \{\omega\}$$

Definition 4.4.5 (ordinals) Define the Von Neumman ordinals, $\mathtt{Ord}$, by saying each ordinal is the well-ordered set of all smaller ordinals. There are two types of ordinals:

- α is a *successor ordinal* if there is some $\beta \in \mathtt{Ord}$ such that $\alpha = \mathsf{succ}(\beta)$.
- α is a *limit ordinal* if it is not a successor ordinal.

Here, too, taking the intersection of all elements in a non-empty set gives their least element.

Theorem 4.4.6 (Ord is too big to be a set) Ord is too big to be a set. We call such an object a *class*.[4]

Proof. Suppose Ord were a set. Then Ord would also be an ordinal. But by the axiom of regularity (2), Ord cannot contain itself. □

Theorem 4.4.7 (transfinite induction) A predicate ϕ is true for all ordinals if

Base case: $\phi(0)$

Inductive step: If, for all α less than some β, $\phi(\alpha)$, we can conclude $\phi(\beta)$.

Proof. Suppose not. Then there is some ordinal $\beta > 0$ that is the smallest ordinal for which ϕ is false. Then, for all $\alpha < \beta$, we know $\phi(\alpha)$. By assumption, the inductive step holds; therefore conclude $\phi(\beta)$, a contradiction. □

4.5 the axiom of choice

We introduce the shorthands $\forall x \in X.\phi(x)$ for $\forall x.x \in X \to \phi(x)$ and $\exists x \in X.\phi(x)$ for $\exists x.x \in X \wedge \phi(x)$.

Definition 4.5.1 (axiom of choice) For any set of sets X, if $\varnothing \notin X$ there is a choice function $f : X \to \bigcup X$ such that $f(X_i) \in X_i$, or

$$\forall X \left(\varnothing \notin X \to \exists f \in \left(\bigcup X \right)^X \forall A \in X.f(A) \in A \right) \tag{4.1}$$

The axiom of choice allows you to make an infinite number of arbitrary choices. In the general case, a description of a choice function or the elements it returns are not possible. This means ZFC contains elements whose existence we assert, although we can never find them. This is the heart of the early 20th century controversy over the axiom of choice.

Definition 4.5.2 (infinite cartesian product) Let I be an index set. If each X_i is a set, we can define their product,

$$\prod_{i \in I} X_i = \left\{ f \in \left(\bigcup_{i \in I} X_i \right)^I : f(i) \in X_i \right\}$$

i.e. the set of functions from I to $\bigcup_{i \in I} X_i$ such that $f(i) \in X_i$.

We can restate the axiom of choice in terms of the above.

Theorem 4.5.3 Let I be an index set. Suppose each X_i is a nonempty set and $X_i \neq X_j$ whenever i and j are distinct. Then the axiom of choice is equivalent to

$$\prod_{i \in I} X_i \neq \varnothing \tag{4.2}$$

[4] There are axioms for class theories analogous to ZFC, but we will not need these, as we will not use many classes

Proof. The set of choice functions on $\bigcup_{i\in I} X_i$ is

$$C = \left\{ f \in \left(\bigcup_{i\in I} X_i \right)^X : f(X_i) \in X_i \right\}$$

whereas

$$P = \prod_{i\in I} X_i = \left\{ f \in \left(\bigcup_{i\in I} X_i \right)^I : f(i) \in X_i \right\}$$

There is a 1-to-1 correspondence between P and C given by converting from f such that $f(X_i) \in X_i$ to an f' such that $f'(i) = f(X_i) \in X_i$. Setting $f'(i) = f(X_i)$ gives this conversion. □

Theorem 4.5.4 (well-ordering theorem) For every set X there is some order $\leqslant$ that makes X well-ordered.

Proof. We will define a 1-to-1 function from a subset of `Ord` to X by transfinite induction. Let f be a choice function for 2^X. This f will pull out successive elements of X, defining a well-order. Define

$$\begin{aligned} X_0 &= X \\ x_0 &= f(X_0) \end{aligned}$$

For α an ordinal, define

$$\begin{aligned} X_{\mathrm{succ}(\alpha)} &= X_\alpha - \{x_\alpha\} \\ x_{\mathrm{succ}(\alpha)} &= f(X_{\mathrm{succ}(\alpha)}) \end{aligned}$$

For β a (nonzero) limit ordinal, define

$$\begin{aligned} X_\beta &= \bigcap_{\alpha<\beta} X_\alpha \\ x_\beta &= f(X_\beta) \end{aligned}$$

Let Ω be the smallest ordinal such that $X_\Omega = \varnothing$. The ordinal Ω must exist, otherwise $n \mapsto x_n$ would be a 1-to-1 function from `Ord` to X, which is impossible by `Ord` is too big to be a set. Thus, the function $n \mapsto x_n$ is a 1-to-1 function from Ω to X. Finally, define the order by

$$x_n \leqslant x_k \leftrightarrow n \leqslant k$$

□

Theorem 4.5.5 (well-ordering theorem $\leftrightarrow$ choice) Instead of assuming the axiom of choice, suppose we use the axioms of Zermelo-Fraenkel set theory and well-ordering theorem. Then we can prove the axiom of choice.

Proof. Consider the set of sets X. Suppose $\varnothing \notin X$. Let $\leqslant$ be a well-ordering on $\bigcup X$, which exists by hypothesis. Define a choice function for X by sending the set $A \in X$ to its least element under $\leqslant$. □

4.6 number systems

We are almost ready to define the familiar number systems in ZFC. In fact, we can as of now but have no way of telling the theory that $1/2$ and $2/4$ are identical objects. Hence we group equivalent representations of a number system into an *equivalence class*.

Definition 4.6.1 (equivalence relation) The 2-ary predicate $\sim$ on the set X is an equivalence relation iff it satisfies

1. Reflexivity: $\forall x \in X . x \sim x$
2. Symmetry: $\forall x, y \in X (x \sim y \to y \sim x)$
3. Transitivity: $\forall x, y, z \in X (x \sim y \wedge y \sim z \to x \sim z)$

Definition 4.6.2 (equivalence classes) Suppose X is a set and $\sim$ is an equivalence relation on X. Then $X/\sim$, equivalence classes of X mod $\sim$, is a set of subsets of X such that

1. Every $x \in X$ is in some $A \in X/\sim$.
2. For all $A \in X$, all elements of $A \in X/\sim$ are $\sim$-equivalent.
3. For all $A, B \in X$, there are no $a \in A$, $b \in B$ such that $a \sim b$.

4.6.1 integers

We can represent integers as pairs of natural numbers (a, b) which will represent the number we think of as $a - b$.

Definition 4.6.3 ($\sim$)

$$(a, b) \sim (x, y) \leftrightarrow a + x = b + y$$

Then

Definition 4.6.4 ($\mathbb{Z}$) Define the integers

$$\mathbb{Z} = \mathbb{N}^2/\sim$$

Using equivalence classes lets us treat different representations of the same number as equal. If we just looked at pairs in $\mathbb{N}^2$, we could say $(0, 3) \equiv (1, 4)$, but not $(0, 3) = (1, 4)$ as they are different pairs. The solution? Define an integer as the set of all pairs that represent it.

Define addition by its action on pairs (a, b) and (x, y):

$$(a, b) + (x, y) = (a + x, b + y)$$

or, in a more suggestive notation,

$$(a - b) + (x - y) = \big(a + x - (b + y)\big)$$

negation by

$$-(a-b) = (b-a)$$

and multiplication by

$$(a-b)\cdot(x-y) = \big(ax+by-(ay+bx)\big)$$

Technically, we defined $+$, $-$ and $\cdot$ for pairs in $\mathbb{N}^2$. To see these define operations on $\mathbb{Z} = \mathbb{N}^2/\sim$, check that equivalent inputs lead to equivalent outputs.

4.6.2 rationals

Rationals will be represented by pairs of an integer (numerator) and a positive integer (denominator). Let $\mathbb{Z}^+$ denote strictly positive integers.

Definition 4.6.5 ($\sim$) For pairs in $\mathbb{Z}\times\mathbb{Z}^+$,

$$(a,b)\sim(x,y) \leftrightarrow ay = bx$$

or, in a more suggestive notation,

$$\frac{a}{b}\sim\frac{x}{y} \leftrightarrow ax = by$$

Then

Definition 4.6.6 ($\mathbb{Q}$)

$$\mathbb{Q} = (\mathbb{Z}\times\mathbb{Z}^+)/\sim$$

where we define addition as

$$\frac{a}{b}+\frac{x}{y} = \frac{ay+bx}{by}$$

negation as

$$-\frac{a}{b} = \frac{-a}{b}$$

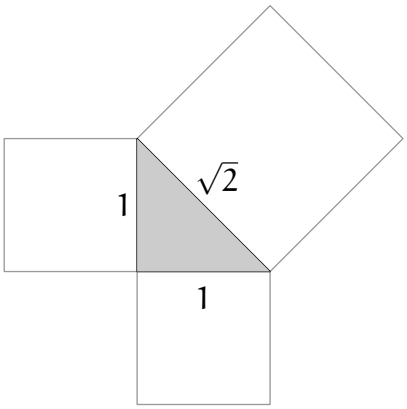
multiplication as

$$\frac{a}{b}\frac{x}{y} = \frac{ax}{by}$$

and the multiplicative inverses as

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

Figure 4.1: Irrational numbers in geometry



4.6.3 reals

Pythagoras believed all numbers were rational. But one day a member of his math-cult stumbled on an irrational number. Pythagoras was so appalled, legend has it he killed the discoverer to suppress this discovery. But mathematics cannot be suppressed. As seen in fig. 4.1, simple geometry confronts us with irrational numbers.

Theorem 4.6.7 ($\sqrt{2}$ is irrational) There is no pair of integers a, b where a/b is in simplest form that satisfy

$$\left(\frac{a}{b}\right)^2 = 2 \tag{4.3}$$

Proof. Suppose there are integers a, b with a/b in simplest form that satisfy eq. (4.3). Then

$$\begin{aligned} \frac{a^2}{b^2} &= 2 \\ a^2 &= 2b^2 \end{aligned} \tag{4.4}$$

so a is even. Then there is some $n \in \mathbb{Z}$ such that $a = 2n$. Substituting $2n$ for a in eq. (4.4) gives

$$\frac{(2n)^2}{b^2} = \frac{4n^2}{b^2} = 2$$

Solving for b gives

$$b^2 = 2n^2$$

so b^2 is even. Recall we're assuming b is an integer. The only way for b^2 to be even when b is an integer is for b to be even. Then a and b are both even, so a/b is not in simplest form, a contradiction. □

This tells us $\mathbb{Q}$ is missing numbers. But so far we only know for sure $\mathbb{Q}$ is missing numbers involving $\sqrt{2}$. What about numbers like π or e that have no obvious connection to $\sqrt{2}$?

Rational numbers can approximate $\sqrt{2}$:

Theorem 4.6.8 (babylonian method) Let x be an approximation for $\sqrt{S}$. We can get a slightly better approximation x' by

$$x' = \frac{x + S/x}{2}$$

Proof. Let ε the approximation's error, *i.e.* $\varepsilon = x - \sqrt{S}$. In other words,

$$\begin{aligned} S &= (x+\varepsilon)^2 \\ S &= x^2 + 2x\varepsilon + \varepsilon^2 \\ S &= x^2 + \varepsilon(2x+\varepsilon) \\ \varepsilon &= \frac{S - x^2}{2x+\varepsilon} \end{aligned} \tag{4.5}$$

If ε is small enough, we can approximate $2x + \varepsilon \approx 2x$. Then eq. (4.5) is approximately

$$\varepsilon \approx \frac{S + x^2}{2x}$$

Now we improve our approximation:

$$\begin{aligned} x' &= x + \varepsilon \\ x' &= x + \frac{S - x^2}{2x} \\ x' &= \frac{2x^2 + S - x^2}{2x} = \frac{S + x^2}{2x} \\ x' &= \frac{x + S/x}{2} \end{aligned}$$

□

Corollary 4.6.9 We can find a sequence of rational numbers that approximates $\sqrt{2}$.

Proof. The babylonian method will give a rational number for x' when x and S are rational.□

Example 4.6.10 If we start with the initial guess $\sqrt{2} \approx 1$, the babylonian method will give

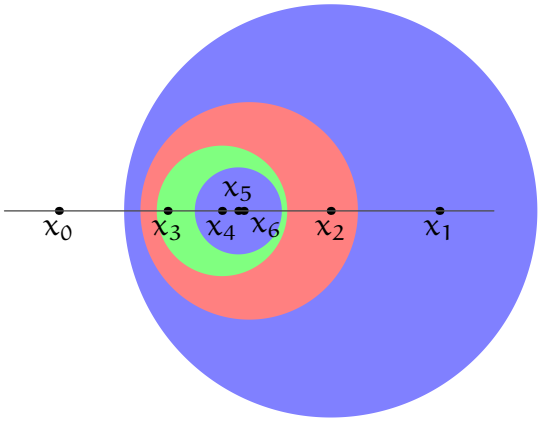
$$\begin{aligned} x_0 &= 1 \\ x_1 &= \frac{1 + 2/1}{2} = 1.5 \\ x_2 &= \frac{1.5 + 2/1.5}{2} = 1.41\bar{6} \\ x_3 &= \frac{1.41\bar{6} + 2/1.41\bar{6}}{2} = 1.4142156862\ldots \\ x_4 &= \frac{1.4142156862\ldots + 2/1.4142156862\ldots}{2} = 1.414213562\ldots \\ &\vdots \end{aligned}$$

Continuing in this fashion, we can construct an infinite sequence $x_0, \ldots, x_n \ldots$ of rationals that approaches $\sqrt{2}$. But we still haven't figured out a definition of irrational numbers in ZFC. We want to find a property that says $x_0, \ldots, x_n \ldots$ looks like an approximation of some number. The key observation is the larger the n, the smaller the adjustments you have to make to get more precision. This is the inspiration for the following definition.

Definition 4.6.11 (approximation-like) A sequence x_n of rational numbers is approximation-like if for any integer P of your choosing there is some N such that all terms after x_N will differ by less than $1/P$, *i.e.* for all $n, m > N$,

$$|x_n - x_m| < \frac{1}{P}$$

Figure 4.2: First six terms of an approximation-like sequence. Once the sequence enters a circle, it never leaves. The circles give an upper bound on the error in the approximation, analogous to the $1/P$ terms.



Definition 4.6.12 ($\sim$) Two approximation-like sequences are $\sim$-equivalent iff the difference in corresponding elements shrinks to 0

$$(x_0, x_1, \ldots x_n \ldots) \sim (y_0, y_1, \ldots y_n, \ldots) \leftrightarrow \lim_{n\to\infty} |x_n - y_n| = 0$$

Definition 4.6.13 ($\mathbb{R}$) Let A be the set of approximation-like sequences of rationals, a subset of $\mathbb{Q}^{\mathbb{N}}$ we can define by specification (ZFC axiom 3). Define the real numbers

$$\mathbb{R} = A/\sim$$

with addition given by

$$(x_0, x_1, \ldots) + (y_0, y_1, \ldots) = (x_0 + y_0, x_1 + y_1, \ldots)$$

negation by

$$-(x_0, x_1, \ldots) = (-x_0, -x_1, \ldots)$$

and multiplication by

$$(x_0, x_1, \dots) \cdot (y_0, y_1, \dots) = (x_0 y_0, x_1 y_1, \dots)$$

For simplicity, we omit the checks that these operations output elements of A, as well as the check that equivalent inputs yield equivalent outputs.

We will show the real numbers are uncountably infinite. This will follow from theorem 4.1.13's proof that $2^{\mathbb{N}}$ is uncountably infinite. Real numbers between 0 and 1 written in binary are infinite binary strings, $2^{\mathbb{N}}$. But there is a problem: rational numbers have two representations. We get around this with the following lemma:

Lemma 4.6.14 Removing a countable number of elements from an uncountable set does not change its size.

Proof. Let X be an uncountable set. Let C be a countable subset. Suppose for the sake of contradiction $X - C$ is countable. Since C is countable, there is a sequence $c_0, c_1, \dots$ that lists all the elements of C. Likewise, there is a sequence $x_0, x_1, \dots$ that lists all of $X - C$. Interleaving the two sequences gives a 1-to-1 correspondence between X and $\mathbb{N}$:

$$\begin{array}{lccccccc} X: & x_0 & c_0 & x_1 & c_1 & x_3 & c_3 & \dots \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & \dots \end{array}$$

But X is uncountable, a contradiction. □

Theorem 4.6.15 Let

$$[0, 1] = \{x \in \mathbb{R} : 0 < x < 1\}$$

There is a 1-to-1 correspondence between $[0, 1]$ and $2^{\mathbb{N}}$.

Proof. There is a 1-to-1 correspondence between $2^{\mathbb{N}}$ and binary representations of $[0, 1]$. To see this, note that a binary representation is an infinite binary string. But this counts every rational number twice. Fortunately, theorem 4.1.11. Then by lemma 4.6.14, we can take out an extra representation of each rational number. This does not change the size, so $[0, 1]$ is the same size as $2^{\mathbb{N}}$. □

Corollary 4.6.16 $(0, 1)$ has the same size as $2^{\mathbb{N}}$.

Corollary 4.6.17 $\mathbb{R}$ has the same size as $2^{\mathbb{N}}$.

Proof. The function

$$\tan\left(\frac{x}{\pi} + \frac{1}{2}\right)$$

is 1-to-1. □

5 model theory

Armed with ZFC, we can take a new approach to investigate predicate logic. In section 3.1, we only studied the symbols and the rules of deduction. The only tool we had to govern the universe was axioms. Now we can crack it open, look inside and change things. Such techniques will be incredibly powerful and provide the key to understanding the theory of first order predicate logic.

To make sense of logic with ZFC, we need to make some sets

Definition 5.0.18 (language) A language is a set of names of constants, functions, and predicates.

Example 5.0.19 The language of ZFC consists of the constant $\varnothing$, the predicate $\in$ and the functions $\bigcup, \bigcap, -$.

Definition 5.0.20 (theory) A theory in a given language is a set of axioms about the constants, predicates, and functions in that language.

A model is an example set that satisfies the axioms of a theory. The natural numbers $\mathbb{N}$ as defined in ZFC models Peano's axioms.

Definition 5.0.21 (model) Consider the language $\mathcal{L}$. A model for the $\mathcal{L}$-theory Φ is the triple (U, d, I).

a set U, the universe

a dictionary function d that translates function and predicate symbols to functions and predicates on U

an interpretation I that translates L-statements to statements about U.

We require that I takes axioms in Φ to true statements. Also, we require[1]

$$\begin{aligned} I(p \wedge q) &= I(p) \wedge I(q) \\ I(p \vee q) &= I(p) \vee I(q) \\ I(\neg p) &= \neg I(p) \\ I(\forall x.p(x)) &= \forall x \in U.(I(p))(x) \\ I(\exists x.p(x)) &= \exists x \in U.(I(p))(y) \end{aligned}$$

Definition 5.0.22 ($\Phi \vdash p$) Define

$$\Phi \vdash p$$

or p is a theorem of Φ iff p can be proved from Φ (set of axioms) using the laws of deduction.

[1] I'm not actually sure of this, but it seems appropriate.

We have referred to consistency a lot. It's time to officially define it

Definition 5.0.23 (consistency) A theory Φ is consistent if for no p

$$\Phi \vdash p \wedge \neg p$$

Theorem 5.0.24 (model $\rightarrow$ consistent) If ZFC is consistent, then any theory Φ with a model in ZFC must be consistent.

Proof. Interpretations let us translate proofs from a theory to the model of the theory. Suppose Φ is a theory with model (U, d, I). Suppose

$$\Phi \vdash p$$

Then I translates the proof of p to a proof of $I(p)$ from the axioms of ZFC. Hence if $\Phi \vdash p \wedge \neg p$, then

$$\text{ZFC} \vdash I(p) \wedge \neg I(p)$$ □

5.1 gödel's constructible universe

This is a model of ZFC with rather interesting properties. Particularly, it can be defined in *Zermelo-Fraenkel set theory without the axiom of choice* (ZF).

Definition 5.1.1 (Gödel's constructible universe) We will build up a universe in layers, starting with $\varnothing$. Each new layer contains all sets defined by a specifying over the sets from the previous layer. First define

$$D(Y) = \left\{\{x : x \in Y \wedge \phi(x, z_1, \ldots, z_n)\} : \phi \text{ is a first order formula, } z_1, \ldots, z_n \in Y\right\}$$

this builds the next layer. Define

$$\begin{aligned} L_0 &= \varnothing \\ L_{\text{succ}\,\alpha} &= D(L_\alpha) \\ L_\beta &= \bigcup_{\alpha<\beta} L_\alpha \\ L &= \bigcup_{\alpha\in \text{Ord}} L_\alpha \end{aligned}$$

where β is a limit ordinal.

Every element in L is defined by a first order formula.

Definition 5.1.2 (birthday) An element $x \in L$ has birthday α if α is the smallest ordinal such that $x \in L_\alpha$.

Lemma 5.1.3 All nonzero birthdays are successor ordinals.

Proof. If $x \in L_\beta$ has nonzero birthday β where β is a limit ordinal, then

$$x \in \bigcup_{\alpha<\beta} L_\alpha$$

in other words, there is some $\alpha < \beta$ such that

$$x \in L_\alpha$$

hence x does not have birthday β, a contradiction. □

Theorem 5.1.4 (L models ZF) The set L models ZF.

Proof.
1. Extensionality—L inherits this axiom from ZF.
2. Regularity—L inherits this from ZF.
3. Specification—this follows from the definition of $L_{\mathsf{succ}(\alpha)}$.
4. Singletons
   Consider the element $x \in L_\alpha$. The formula
   $$\phi(y, z) \leftrightarrow \forall s \in y(s = z)$$
   defines $\{x\}$ when $z = x$. Hence $\{x\} \in L_{\alpha+1}$.
5. Union—$\bigcup z$ is defined by the forumla
   $$\phi(u, z) \leftrightarrow \forall y(y \in u \leftrightarrow \exists x \in z.y \in x)$$
6. Replacement—replacement is a recipe for constructing a new set with a predicate. Hence L is closed under replacement.
7. Infinity—L_1 contains $\varnothing$. If n in $L_{\mathsf{succ}(n)}$, then $\mathsf{succ}(n)$ is in L_{n+2}. Hence, L_ω contains $\mathbb{N}$.
8. Powerset—the formula
   $$\phi(x, z) \leftrightarrow \forall y(y \in x \leftrightarrow y \subseteq z)$$
   defines the powerset, x, of z. □

Theorem 5.1.5 (well-ordering in L) The well-ordering theorem holds in L.

Proof. We can actually well-order L by transfinite induction. An element in $L_{\mathsf{succ}(\alpha)}$ is uniquely determined by its defining formula $\phi(x, z_1, \ldots, z_n)$ and the choice of $z_1, \ldots, z_n \in L_\alpha$.

1. Base case: L_0 is vacuously well-ordered.

2. Successor ordinals:
   Suppose L_α is well-ordered. Then we can well-order the set of finite sequences of elements in L_α with the dictionary order, *i.e.* $x_1, x_2, \ldots x_n < y_1, y_2, \ldots y_m$ if $x_1 < y_1$, or $x_1 = y_1$ and $x_2 < y_2$, or $(x_1, x_2) = (y_1, y_2)$ and $x_3 < x_4$...and if there is a tie, *i.e.* $x_1 = y_1 \ldots x_{\min(m,n)} = y_{\min(m,n)}$ the shorter sequence is smaller. Let $\texttt{finseq}(L_\alpha)$ denote the finite sequences of L_α

   Every element of $L_{\mathrm{succ}(\alpha)}$ is uniquely determined by its defining formula and the sequence of $z_1 \ldots z_n \in L_\alpha$. Using a godel numbering, we can say the elements of $L_{\mathrm{succ}(\alpha)}$ are in 1-to-1 correspondence with $\mathbb{N} \times \texttt{finseq}(L_\alpha)$, which the dictionary order well-orders.

3. Limit ordinals:
   Suppose β is a limit ordinal and for all $\alpha < \beta$, the set L_α is well-ordered. We define a well-order $\leqslant$ on L_β as follows. Consider $x, y \in L_\beta$. Suppose $x \in L_n$ and $y \in L_k$ where n and k are successor ordinals. If $n = k$, define $x \leqslant y$ iff the order defined in (2) says so. Otherwise, when $n < k$, define $x \leqslant y$. □

Corollary 5.1.6 ZFC is consistent if ZF is consistent.

5.2 gödel's completeness theorem

Definition 5.2.1 (maximally consistent) A theory Φ over language $\mathcal{L}$ is maximally consistent iff

Φ is consistent

for every $\mathcal{L}$-sentence p, either $p \in \Phi$ or $\neg p \in \Phi$.

Definition 5.2.2 (witnesses) A theory Φ over language $\mathcal{L}$ has witnesses if every statement of the form $\exists x.\phi(x)$ has a corresponding term, a witness if you will, w such that

$$\big(\exists x.\phi(x) \to \phi(w)\big) \in \Phi$$

Theorem 5.2.3 (model existence theorem) Every maximally consistent theory Φ with witnesses has a model in ZFC.[2]

Proof. We can turn Φ into a model of Φ. We're essentially repackaging first order logic's deductive system as a model. Define the equivalence relation $\sim$ by

$$x \sim y \text{ iff } (x \leftrightarrow y) \in \Phi$$

Define the universe

$$U = \Phi/\sim$$

[2] Every maximally consistent Φ can be given witnesses as so long as we add a constant symbol to act as a witness for each existential statement.

For each constant symbol c in $\mathcal{L}$, define $d(c)$ to be the equivalence class of c in U. For each function symbol f in $\mathcal{L}$, define $d(f)$ as the function sending the equivalence class of $x \in U$ to the equivalence class of $f(x) \in U$. For each relation symbol R in $\mathcal{L}$, define

$$(d(R))(x) \leftrightarrow \big(R(x) \in \Phi\big)$$

Define the interpretation $I(\phi)$ iff $\phi \in \Phi$. Then (U, d, I) is a model of Φ. □

Corollary 5.2.4 (Gödel's completeness theorem) Assume ZFC is consistent. Then a theory Φ is consistent iff it has a model in ZFC. In particular,

$$\Phi \vdash \phi$$

iff ϕ is true in every model of Φ.

This gives us a new approach to understanding logical deduction.

Theorem 5.2.5 (compactness theorem) A theory Φ has a model iff every finite subtheory $F \subseteq \Phi$ has a model.

Proof. By Gödel's completeness theorem, Φ has a model iff it is consistent. Suppose Φ is not consistent. Then we can prove a contradiction starting from Φ. A proof has finitely many steps, so it can only use finitely many axioms. Thus, there is some finite subtheory $F \subseteq \Phi$ such that the axioms F leads to a contradiction. Hence, F has no model. □

5.3 löwenheim–skolem theorem

Definition 5.3.1 (Skolem function) Consider a model $M = (U, d, I)$. Suppose M models the statement

$$\forall x_0, \ldots, x_n \exists y. \phi(x_0, \ldots, x_n, y)$$

Then there is some function $f_y : U^n \to U$ that gives us such a y:

$$\phi\big(f_y(x_0, \ldots, x_n), x_0, \ldots, x_n\big)$$

Such a f_y is a Skolem function.

Theorem 5.3.2 (downward Löwenheim-Skolem) Every theory with an infinite model has a countable model.

Proof. Let Φ be a theory. Suppose Φ has infinite model M. Let S be the collection of Skolem functions for Φ. Let M_0 be a countable subset of M. Then define

$$M_{\mathrm{succ}(n)} = \bigcup_{f \in S} f(M_n) \cup M_m$$

Let

$$M_\omega = \bigcup_{n \in \mathbb{N}} M_n$$

Then for each $f \in S$, conclude $f(M_\omega) \subseteq M_\omega$. Hence M_ω models Φ. But M_ω is a countable union of countable sets; thus M_ω is countable. □

An implication of this is Skolem's paradox: there is a countable model of ZFC that models the statement $2^{\mathbb{N}}$ is uncountable.

Theorem 5.3.3 (upward Löwenheim-Skolem) Every theorem with an infinite model has a model that is arbitrarily large.

Proof. Suppose Φ is a theory over language $\mathcal{L}$ with infinite model M. By downward Löwenheim-Skolem, we can assume M is countable. Pick the ordinal α. We will construct a model M' with a subset the same size as α. Suppose x_n is a symbol not in the language $\mathcal{L}$ for each $n < \alpha$. Define

$$\mathcal{L}' = \mathcal{L} \cup \{x_n : n < \alpha\}$$
$$\Phi' = \Phi \cup \{x_i \neq x_j : i < j < \alpha\}$$

Every finite subset of Φ' has a model. By the compactness theorem, Φ' has a model. Call it M'. Then M' contains $d(x_n)$ for each $n \in \alpha$. □

Bibliography

[Ang15] Devlin's Angle. *The hidden math behind* Alice in Wonderland. 2015. URL: https://www.maa.org/external_archive/devlin/devlin_03_10.html.

[Mat] Story of Mathematics. *20th Century Mathematics—Russel and Whitehead*. URL: http://www.storyofmathematics.com/20th_russell.html.

[Wik15a] Wikipedia. *Angle trisection*. 2015. URL: https://en.wikipedia.org/wiki/Angle_trisection.

[Wik15b] Wikipedia. *De Morgan's laws*. 2015. URL: https://en.wikipedia.org/wiki/De_Morgan%27s_laws.

[Wik15c] Wikipedia. *Hilbert's Program*. 2015. URL: https://en.wikipedia.org/wiki/Hilbert%27s_program.

[Wik15d] Wikipedia. *Peano axioms*. 2015. URL: https://en.wikipedia.org/wiki/Peano_axioms.

[Wik15e] Wikipedia. *Problem of multiple generality*. 2015. URL: https://en.wikipedia.org/wiki/Problem_of_multiple_generality.

[Wik15f] Wikipedia. *Proof sketch for Gödel's first incompleteness theorem*. 2015. URL: https://en.wikipedia.org/wiki/Proof_sketch_for_G%C3%B6del%27s_first_incompleteness_theorem.