Mathematical Logic:
The Rules of Mathematics and How to Break Them

Mark Schachner | September - October 2025

Day 1: 16 September

Today: Introductions and fun with paradoxes.

Seminar logistics:

- **Title**: Mathematical Logic: the Rules of Mathematics and How to Break Them
- **Instructor**: Mark Schachner
- **Email**: mjs623@cornell.edu

ACTIVITY: Getting to know each other.

On your notecard, please write down:

- your preferred name and how to pronounce it;
- your pronouns;
- your year; and
- a fact about you -or- a question for me.

Share facts and questions.

ACTIVITY: Big number challenge.

Everyone gets 60 seconds to write down the largest number they can think of on their notecard. Rules:

1. You must **uniquely specify an integer**.

   Not allowed: ∞, "bazillion", "the biggest number", etc.

2. You cannot make reference to other students' numbers or cards.

   Not allowed: "the biggest of all the other numbers, plus 1", etc.

Consider the following number:

> The smallest number that cannot be uniquely specified on this notecard.

Discuss.

ACTIVITY: The hypergame paradox.

For our purposes a "game" is always played between two players, who alternate taking turns until the game is over. Examples: chess, tic-tac-toe, etc.

> **Definition.** A *finite game* is a game which always ends in a finite number of turns.

Most games are finite, but some are not finite: consider the (somewhat silly) game where each player names a number on their turn, and the first player to name the number 0 loses.

> **Definition.** The game *hypergame* is played as follows:
>
> - the first player names any finite game;
> - the two players then play that game; and
> - the outcome of the played finite game is the outcome of the hypergame.
>
> For example, if the first player names tic-tac-toe, then the two players play tic-tac-toe, and the outcome of the played tic-tac-toe game is the outcome of the hypergame.

> **Question.** *Is hypergame a finite game?*

Discuss.

> **Key Idea.** *Many questions in mathematics can only be answered by thinking carefully about what is meant by the objects in question.*

In the above cases:

- What does it mean to "uniquely specify an integer"?
- What is a "game"?

Mathematical logic is all about dealing with these sorts of questions.

Day 2: 18 September

Today: Euclid and the parallel postulate.

Link: https://mathcs.clarku.edu/~djoyce/elements/elements.html

Euclid's axioms for geometry:

1. Any two points can be connected by a line.
2. Any line can be extended indefinitely in both directions.
3. A circle can be drawn with any center and any radius.
4. All right angles are equal.
5. (The parallel postulate) Given a line and a point not on the line, there is exactly one line through the point parallel to the given line.

ACTIVITY: Book I, Propositions 1, 9.

Prove the following:

1. Given a line segment AB, there exists an equilateral triangle with AB as one of its sides.
2. Given any angle, there exists a line segment dividing it into two equal angles.

If you finish early, look carefully at your proofs. Are you using anything other than the five axioms?

The first four axioms seem more "obvious" than the fifth. Can we prove the parallel postulate from the first four axioms? More to the point, how do we prove whether a statement is provable?

Discuss.

Definition. Given a list of axioms, a *model* is a structure that satisfies all of the axioms.

Models of Euclid's axioms:

- The real plane.
- The Gans disk.

Key Idea. *If we can build a model of a list of axioms in which a statement is false, then the statement is* ***not*** *provable from the axioms.*

ACTIVITY: Independence of the parallel postulate.

Can you build a model of the first four axioms in which the parallel postulate is false?

Day 3: 22 September

Today: Set theory and the foundational crisis.

The discovery of independence phenomena led to natural questions about mathematics in general:

- Is there a list of axioms which governs all of mathematics?
- Can a list of axioms be found which does not suffer from independence phenomena?

Struggles over the answers to these questions led to the "foundational crisis" in mathematics in the late 19th century and early 20th century. In the end, set theory emerged as the consensus for the foundation of mathematics.

Definition (Mathematical objects as sets)**.** Well-known mathematical objects can be built up from sets in several ways. Here is one way:

- The ordered pair (A, B) can be encoded as the set
$$\{A, \{A, B\}\}.$$
- A function f from a set A to a set B can be encoded as the set
$$\{(x, f(x)) \mid x \in A\}.$$
- We can build natural numbers by setting 0 to be the empty set, and then defining $n = \{0, 1, 2, \ldots, n-1\}$.
- Integers can be defined as pairs of natural numbers. The pair (a, b) represents the integer $a - b$. Two pairs (a, b) and (c, d) represent the same integer if and only if $a - b = c - d$, i.e. if and only if $a + d = b + c$.
- Rational numbers can then be defined as pairs of integers. The pair (a, b) represents the rational number a/b. Two pairs (a, b) and (c, d) represent the same rational number if and only if $ad = bc$, i.e. if and only if $a = c$ and $b = d$.
- Real numbers can then be defined as sets of rational numbers. Search "Dedekind cuts" for one way to do this.

But even set theory was not without its own problems:

ACTIVITY: Russell's paradox, in three forms.

Consider the following situations.

1. In a small town, there is a barber who cuts hair for free, but only for those who do not cut their own hair. Does the barber cut their own hair?
2. Some words describe themselves: for example, "short" is a short word, and "pentasyllabic" is a pentasyllabic word. Other words do not describe themselves: for example, "long" is not a long word, and "monosyllabic" is not a monosyllabic word. Let's call a word "heterological" if it does not describe itself. Is "heterological" a heterological word?
3. The Meta-dictionary is a list of all dictionaries that do not list themselves as entries. Does the Meta-dictionary list itself as an entry?

What do these situations have in common? *Discuss.*

Russell's paradox showed that not every collection of objects can be a set. So which collections can be sets?

Day 4: 25 September

Today: Axioms for sets.

First, some constructions of sets you may have seen before.

- The *empty set* is the unique set with no elements.
- Given any two sets A and B, the *union* of A and B is the set of all elements which are in A or B.
- Given any two sets A and B, the *intersection* of A and B is the set of all elements which are in both A and B.
- Given any two sets A and B, the *cartesian product* of A and B is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. More generally, the *cartesian product* of a family of sets $\langle A_i : i \in I \rangle$ is the set of all sequences $\langle a_i \in A_i : i \in I \rangle$.
- Given any set A, the *power set* of A is the set of all subsets of A.

ACTIVITY: Rules for sets.

In groups, write down a list of rules for building sets. Your axioms should be able to build the following objects:

- The empty set.
- Unions, intersections, cartesian products, and functions.
- Sets like $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Here are some ideas to get you started:

- You need to be able to build *something*. So you'll need an axiom which asserts the existence of at least one set.
- It may seem obvious that if A and B are sets, then the set $\{A, B\}$ is a set. But how do you know that $\{A, B\}$ is a set? You'll need an axiom which asserts the existence of sets of the form $\{A, B\}$. Think about this and other "obvious" facts which might require axioms.
- You'll need an axiom which asserts the existence of a set of all sets which satisfy a given property. But beware of Russell's paradox!

The generally accepted rules for building sets are called ZFC: the Zermelo-Fraenkel axioms plus the axiom of choice. They start with some "obvious" facts:

- Two sets are the same if they have the same elements.
- There exists an infinite set.
- If A and B are sets, then the set $\{A, B\}$ is a set.
- If A is a set, then the set of all subsets of A is a set.
- The union of a family of sets is a set.

Then there are a few less obvious axioms:

- (Foundation) Every non-empty set A has an element B which is disjoint from A.
- (Replacement) If A is a set and f is a function, then the image of A under f is a set.
- (Separation) If A is a set and P is a property, then the set of all elements of A which satisfy P is a set.
- (Choice) The cartesian product of a non-empty family of nonempty sets is nonempty.

We'll return to these later.

Day 5: 29 September

Today: Cardinality.

We'll use the following notations for sets:

- $\mathbb{N}$: all natural numbers.
- $\mathbb{Z}$: all integers.
- $\mathbb{Q}$: all rational numbers.
- $\mathbb{R}$: all real numbers.

We'll also make use of *set builder notation*, writing $\{x \in X : x \text{ has property } P\}$ for the set of all elements of X which have property P.

ACTIVITY: Counting infinite sets.

For each of the following pairs of sets, determine which set has more elements, or if they have the same number of elements. (No proofs needed; feel free to go by vibes.)

1. The set of all matches in a single-elimination tennis tournament; the set of all players who lose at least one match.
2. $\{n \in \mathbb{N} : n \text{ is even}\}$; $\{n \in \mathbb{N} : n \text{ is odd}\}$.
3. $\{n \in \mathbb{N} : n \text{ is even}\}$; $\mathbb{N}$.
4. $\mathbb{N}$; $\mathbb{Z}$.
5. $\mathbb{N}$; $\mathbb{Q}$.
6. $\mathbb{N}$; $\{A \subseteq \mathbb{N} : A \text{ is finite}\}$.

Discuss.

Definition. The *cardinality* of a set A is the number of elements in A, written $|A|$. If A is infinite we have special notation for $|A|$: for instance we write $\aleph_0$ for the cardinality of $\mathbb{N}$.
We say that A and B have the same cardinality if the elements of A and B can be paired off exactly in a one-to-one correspondence.

Even though the sets look different, the cardinalities of all the above sets– $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, finite subsets of $\mathbb{N}$, etc. – are the same.
However, Cantor showed that the cardinality of $\mathbb{R}$ is strictly greater than the cardinality of $\mathbb{N}$:

ACTIVITY: Cantor's diagonalization argument.

1. Suppose we have a correspondence between $\mathbb{N}$ and $\mathbb{R}$. Maybe the first few pairs look like this:

$$\begin{aligned}
0 &\leftrightarrow 0.434828947967145986432109876543\ldots \\
1 &\leftrightarrow 0.343485291840175302918401753029\ldots \\
2 &\leftrightarrow 0.848274718529184017530291840175\ldots \\
3 &\leftrightarrow 0.233457382918401753029184017530\ldots \\
&\vdots
\end{aligned}$$

   Can you build a real number x which is not in the list?

2. Suppose we have a correspondence between $\mathbb{N}$ and the *power set* of $\mathbb{N}$, i.e. the set of all subsets of $\mathbb{N}$. Maybe the first few pairs look like this:

$$\begin{aligned}
0 &\leftrightarrow \{n \in \mathbb{N} : n \text{ is even}\} \\
1 &\leftrightarrow \{n \in \mathbb{N} : n \text{ is odd}\} \\
2 &\leftrightarrow \{7, 2\} \\
3 &\leftrightarrow \{n \in \mathbb{N} : n \text{ is a multiple of } 3\} \\
&\vdots
\end{aligned}$$

   Can you build a subset A of $\mathbb{N}$ which is not in the list?

3. Suppose we have a correspondence between $\mathbb{N}$ and the set of all functions from $\mathbb{N}$ to $\mathbb{N}$. Maybe the first few pairs look like this:

$$\begin{aligned}
0 &\leftrightarrow f_0(n) = n \\
1 &\leftrightarrow f_1(n) = n + 1 \\
2 &\leftrightarrow f_2(n) = 2n \\
3 &\leftrightarrow f_3(n) = 2n + 1 \\
&\vdots
\end{aligned}$$

   Can you build a function f from $\mathbb{N}$ to $\mathbb{N}$ which is not in the list?

The sets $\mathbb{R}$, the power set of $\mathbb{N}$, and the set of all functions from $\mathbb{N}$ to $\mathbb{N}$ all have the same cardinality too. We write this cardinality as $2^{\aleph_0}$, or sometimes $\mathfrak{c}$. What we've just seen is that $\aleph_0 < 2^{\aleph_0}$.

Repeating this argument, we can show that there are infinitely many infinite cardinalities!

Day 6: 1 October

Today: Ordinals.

Last time we talked about cardinalities, which are one way to think about infinity. Ordinals are another way.

ACTIVITY: Big number challenge, part 2.

Everyone gets 60 seconds to write down the largest number they can think of on their notecard. Rules:

1. Infinity is now allowed! So is "infinity plus one", which is bigger than infinity. So is "infinity plus infinity", which is bigger than infinity plus one. And so on.
2. No reference to other students' cards, or to the challenge itself.

Recall how we defined the natural numbers:

- 0 is the empty set.
- $n+1 = n \cup \{n\} = \{0, 1, 2, \ldots, n\}$.

We can then write $\mathbb{N}$ as the set of all of these sets:

$$\mathbb{N} = \{0, \{0\}, \{0, \{0\}\}, \{0, \{0\}, \{0, \{0\}\}\}, \ldots\}.$$

Written this way, we call this set ω. And then we can continue, writing $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}$, and so on. We get numbers like:

- $\omega \cdot 2 = \{0, 1, \ldots, \omega, \omega + 1, \ldots\}$.
- $\omega^2 = \{0, 1, \ldots, \omega, \omega + 1, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \ldots\}$.
- $\omega^3 = \{0, 1, \ldots, \omega, \omega + 1, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \ldots, \omega^2, \omega^2 + 1, \ldots, \omega^2 \cdot 2, \omega^2 \cdot 2 + 1, \ldots\}$.
- $\omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}$, etc.

Key Idea. *Every ordinal is built as the set of all smaller ordinals. Some ordinals are "successors", like $\omega^2 + 1$, while others are "limits", like $\omega \cdot 4$.*

As sets, all the ordinals we've seen so far are countable, i.e., their cardinality is $\aleph_0$.
But there are uncountable ordinals! For example, the ordinal ω_1 is the set of all countable ordinals. We write $|\omega_1| = \aleph_1$. And so on: $\aleph_\alpha$ is defined as the cardinality of ω_α.

ACTIVITY: The fast-growing hierarchy.

Ordinals can be used to write down enormous finite numbers. Define a sequence of functions as follows:

- $f_0(n) = n + 1$.
- For any successor ordinal $\alpha + 1$,

  $$f_{\alpha+1}(n) = f_\alpha(f_\alpha(\cdots f_\alpha(n)\cdots))$$

  where there are n copies of f_α.
- If λ is a limit ordinal, written as

  $$\lambda = \lim\{\beta_0, \beta_1, \beta_2, \ldots\},$$

  then $f_\lambda(n) = f_{\beta_n}(n)$.

Calculate the following, or give up:

- $f_3(n)$ for $n = 0, 1, 2, 3, 4$.
- $f_\omega(n)$ for $n = 0, 1, 2, 3, 4$.
- $f_{\omega\cdot 2}(n)$ for $n = 0, 1, 2, 3, 4$.
- $f_{\omega^2}(n)$ for $n = 0, 1, 2, 3, 4$.

Day 7: 6 October

Today: The axiom of choice.

The axiom of choice depends on the following definition:

Definition. Given a family of sets $\langle A_i : i \in I \rangle$, the *cartesian product* is the set $\prod_{i \in I} A_i$ of all tuples $\langle a_i \in A_i : i \in I \rangle$.

Elements of cartesian products can be thought of as choices: for example, if each A_i is a set of clothing items, then the cartesian product is the set of all possible outfits.
The axiom of choice is the following statement:

> If each A_i is non-empty, then the cartesian product $\prod_{i \in I} A_i$ is non-empty.

In this form, the axiom looks obvious. But it already has some nontrivial consequences!

ACTIVITY: The hat game.

1. There are 10 people in a room, sitting in a straight line. Each person is wearing a hat, and each hat is either red or blue. No one can see their own hat, but they can see the hats of the people in front of them. From front to back, each person must guess the color of their own hat. Find a strategy which guarantees that 9 of the people guess correctly.
2. In a much bigger room, there are infinitely many people, sitting in a straight line. Each person is wearing a hat and can see the hats of the people in front of them. But this time the hats can be any color at all. Can you find a strategy which guarantees that all but finitely many people guess correctly?

The second task sounds impossible, but it's doable using the axiom of choice:

- Say two hat sequences are *basically the same* if after a finite number of steps they are identical.
- Then for any hat sequence H, let S_H be the set of all basically the same hat sequences. This is nonempty, so choice lets us pick a favorite hat sequence from each S_H.
- The players' strategy is to guess the color of their own hat based on the favorite hat sequence they see.

Some other unexpected consequences of the axiom of choice:

- The *Banach-Tarski paradox*: a ball can be decomposed into finitely many pieces which can be reassembled into two balls of the same size.
- The real numbers can be well-ordered.

However, without the axiom of choice, the situation is even worse:

- There can be two sets A and B such that neither $|A| \leq |B|$ nor $|B| \leq |A|$.
- There can be an infinite set which cannot be split into two infinite subsets.
- There can be a set which can be split into more parts than it has elements.

The axiom of choice is now accepted as a fundamental principle of mathematics, despite its controversial status in the early 20th century.

Day 8: 8 October

Today: Beyond ZFC.

The goal of writing down a list of axioms like ZFC was to build a foundation for mathematics which could avoid paradoxes while still answering any mathematical question one might ask. For now, we'll assume ZFC does not lead to paradoxes. But, as we've hinted at, there are some questions which ZFC cannot answer.

ACTIVITY: The continuum hypothesis.

We've seen that the cardinality of the set of real numbers is larger than the cardinality of the set of natural numbers. That is,

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

A natural question is whether there's a set "in between" the natural numbers and the real numbers. That is, can you find a set of real numbers A such that $\aleph_0 < |A| < \mathfrak{c}$? *Discuss.*

What might such a set look like? Georg Cantor, working in the late 1800s, thought that there was no such set, and proposed the following conjecture:

Conjecture (The continuum hypothesis)**.** *There is no set A such that $\aleph_0 < |A| < \mathfrak{c}$.*

Cantor proved that there is no such set A which is "nice" in a specific sense. But he was unable to prove the full continuum hypothesis. And in fact, it turns out that the continuum hypothesis is independent of ZFC, meaning that it cannot be proven or disproven from ZFC alone!
While this startled the mathematical community at the time, it turns out that there are many statements which are independent of ZFC. However, most of these have a similar flavor to the continuum hypothesis: their statements are very infinitary in nature, and seem to have little to do with the work of everyday mathematicians. So the question became: are there any *relevant* statements which are independent of ZFC?

ACTIVITY: Independent statements.

Each of the following statements is independent of ZFC. Your group should decide whether it "feels" like it should be true, false, or neither.

1. If a set X is smaller than a set Y, then X has fewer subsets than Y.
2. If we assign one of countably many colors to each real number, then there are numbers a, b, c, d all the same color such that $a + b = c + d$.
3. Call a subset of the plane a "cloud around a point" if every line through the point intersects the subset in at most finitely many points. Then the plane can be covered by 3 clouds.
4. For every function f from $\mathbb{R}$ to the set of countable subsets of $\mathbb{R}$, there are real numbers x, y such that $x \notin f(y)$ and $y \notin f(x)$.

Discuss.

Day 9: 10 October

Today: Model theory.

Recall the definition of a *model*:

Definition. Given a list of axioms, a *model* is a structure that satisfies all of the axioms.

ACTIVITY: Axioms for cycle graphs.

A graph is a set of points connected by edges. We call a graph a *cycle graph* if the points are connected by edges in a cycle.

1. Write down a sentence which is true in the cycle graph with 3 points, but false in the cycle graph with 4 points.
2. Write down a sentence which is true in cycle graphs, but false in non-cycle graphs.
3. Can you write down a list of "axioms for cycle graphs"? Meaning, a list of sentences which are all true precisely if a graph is a cycle graph.

On day 2, we saw that an important way to show that a statement is not provable from a list of axioms is to build a model of the axioms in which the statement is false. It turns out that this is the *only* way to show that a statement is not provable from a list of axioms!

Theorem (Gödel's completeness theorem)**.** *A statement is provable from a list of axioms if and only if it is true in all models of the axioms.*

Proving this is beyond our scope, but we can think about some consequences.

ACTIVITY: The compactness theorem.

Start with the "language of the natural numbers". We're going to add a new symbol N which represents some number. Consider the following set of axioms:

$$A = \{N > 0, N > 1, N > 2, \ldots\}.$$

1. Is A consistent? That is, can you build a model in which all of the axioms in A are true?
2. Suppose A is not consistent. Then there is a proof of a contradiction from the axioms in A. Can this proof use all of the axioms in A?
3. Let A' be a finite subset of A. Is A' consistent? What does this say about the case when A' is the axioms in A which were used in the proof of the contradiction?
4. Now look back at question 1. Is your answer the same?

This activity shows that the usual "first-order" theory of the natural numbers has certain "non-standard" models, which have elements that behave like infinite numbers. Similar situations puzzled set theorists, but ultimately became seen as more of a feature than a bug.

Day 10: 15 October

Today: Computability I.

So far, we've spent most of our time thinking about the abstract limits of provability. This week, we'll shift gears and think about the more concrete idea of *computability*.
Computability is all about the notion of algorithm: a a procedure, laid out in a finite list of steps, for performing some operation.
Examples:

- Algorithms for arithmetic: multiplication, long division, etc.
- The procedure for factoring / solving quadratic equations is an algorithm.
- Programs written in a programming language count as well.

As a nonexample, many activities we've done were not phrased as algorithms: in thinking creatively about axioms and proofs, we used open-ended thought rather than a fixed procedure.
Whenever we're thinking about computability, we need to fix an alphabet and a "model of computation". Our alphabet for today will just be binary: the set $\{0,1\}$. Our first model of computation will be the following.

Definition. A *deterministic finite automaton*, or DFA, comes with a finite list of states and a list of rules for moving between them. Each state has an arrow to a single other state for each of 0,1. There is also a special initial state and a set of final states.

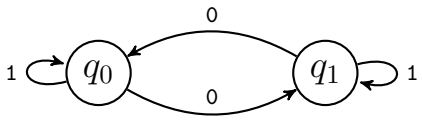
The procedure for running a DFA on an input string goes as follows.

- Start at the initial state.
- For each symbol in the input string, follow the arrow from the current state to the next state.
- If you end at a final state, then the input string is accepted. Otherwise, it is rejected.

The set of strings accepted by the DFA is called the *language* recognized by the DFA.

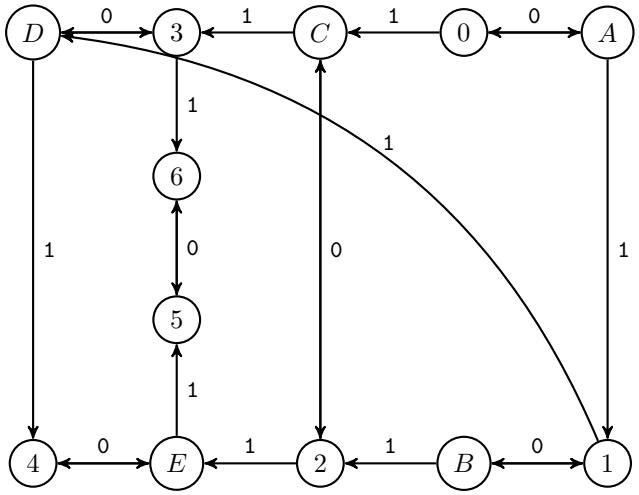
ACTIVITY: Running a DFA.

Consider the following DFA, with initial state q_0 and final state q_1:



Run this DFA on the input strings `000001`, `1010`, and `11111`. Can you determine the language recognized by the DFA?

While DFAs are a weak model, they can perform many familiar computations. For example, the following DFA adds together two 2-bit binary numbers:



(Here the initial node is 0, and all the numbered states are final.)

ACTIVITY: Creating DFAs.

Write down DFA's which recognize the following languages:

1. The language of all strings which contain at least one 0.
2. The language of all strings which contain no 1s.
3. The language of all strings of length 5.
4. The language of all strings of odd length.
5. The language of all strings which start and end with the same symbol.

Can you think of a language which might be difficult to recognize by a DFA? _____

Day 11: 17 October

Today: Computability II.

Last time we used DFAs as a simple model of computation. Now we'll move to a more powerful model: programs in a programming language.
Which programming language? In fact, according to the *Church-Turing thesis*, it basically doesn't matter!

> **Theorem** (Church-Turing thesis)**.** *Any strong enough "reasonable" model of computation can be simulated by any other strong enough "reasonable" model of computation.*

This is not really a theorem, since it's not clear what "reasonable" or "strong enough" means. (DFAs don't count as strong enough.) But the point is that most models of computation– including all mainstream programming languages– are equivalent.
The remarkable fact we'll focus on today is that there are some problems which are *uncomputable*: there is no program which can solve them. The classic example is the *halting problem*:

> **Definition** (The halting problem)**.** The *halting problem* is the problem of determining whether a given program stops running eventually on a given input.

ACTIVITY: The halting problem is uncomputable.

Suppose there is a program H which solves the halting problem. So H takes as input a program P and an input I, and outputs "stuck" if P runs forever on I, and "not stuck" otherwise. Consider also the following programs:

- D: (The duplicator) Take an input I and output two copies of I.
- N: (The negator) On input "stuck", output "not stuck", and on input "not stuck", run an infinite loop (i.e., get stuck).

We can stick these together to make a new program X:

- X takes as input a program P.
- X runs D on P, and feeds the two outputs to H.
- Then H passes its output to N.
- And N outputs the final answer.

The question is: what happens when we run X on input X?

- First, X runs D on X, which gives us two copies of X. These outputs are fed to H.
- Then H runs X on X. It either says "stuck" or "not stuck".
- If H says "stuck", then N outputs "not stuck", so X doesn't get stuck. But H said "stuck"!
- If instead H says "not stuck", then N runs an infinite loop, so X gets stuck. But H said "not stuck"!

This is a contradiction, since H was supposed to always solve the halting problem.
Therefore, the halting problem ifs uncomputable.

Does this proof seem familiar? _____

Day 12: 21 October

Today: Type theory and alternate foundations.

This week we're back to thinking about foundations of mathematics. We previously talked about using sets to represent mathematical objects. But there are other ways to do this as well. One way is to use *type theory*.

ACTIVITY: Russell's resolution of his paradox.

Recall the paradoxical set involved in Russell's paradox:

$$R = \{x \mid x \text{ is a set and } x \notin x\}.$$

One way we might try to resolve this is to introduce "types" of sets:

- The empty set has type 0.
- If A is a set of sets of type n, then A has type $n+1$.
- And so on.

Recall the standard definition of natural numbers: $0 = \emptyset, 1 = \{0\}, 2 = \{0,1\}, 3 = \{0,1,2\}, \ldots$. What is the type of n? What is the type of the set of all natural numbers?
Can the set R be given a type? Why or why not?

Type theory resolves paradoxes by requiring that expressions be "well-typed". Restricting the allowed expressions limits the power of the system somewhat, but it keeps the system consistent.
We can go even further and take as fundamental the types themselves and the functions between them. One way to do this is the *simply-typed lambda calculus*, created by Alonzo Church.

Definition (Simply-typed lambda calculus)**.**
Expressions in the simply-typed lambda calculus are built as follows.

- For types τ and σ, the notation $\tau \to \sigma$ is expresses "the type of functions from τ to σ."
- For a term $e : \tau \to \sigma$ and a term $x : \tau$, the notation $e\,x$ is an expression, read as "the application of e to x." The type of $e\,x$ is σ.
- If e is a term of type $\tau \to \sigma$ and x is a variable, the notation $\lambda x.e$ is an expression, read as "the function which applies e to x." The type of $\lambda x.e$ is $\tau \to \sigma$.

Some examples:

- The term $I = \lambda x.x$ encodes the identity function: $I\,x = x$ for all x.
- For any x, we can define the constant function $K\,x = \lambda y.x$ which always returns x. Abstracting further, we can define the term $K = \lambda x.\lambda y.x$ which encodes all constant functions.
- Function composition can be encoded as $B = \lambda f.\lambda g.\lambda x.f\,(g\,x)$ which applies g to x and then applies f to the result.

ACTIVITY: Church numerals.

If lambda calculus is to be used as a foundation for mathematics, it needs to be able to represent basic mathematical objects. Can you think of a system for representing natural numbers in lambda calculus?

Church did this as follows:

- $0 = \lambda f.\lambda x.x$
- $1 = \lambda f.\lambda x.f\ x$
- $2 = \lambda f.\lambda x.f\ (f\ x)$
- $3 = \lambda f.\lambda x.f\ (f\ (f\ x))$
- And so on.

The idea is that n is the function which applies f to x n times.
Can you think of ways to encode other mathematical objects in lambda calculus? _____

Day 13: 23 October

Today: Philosophy day.

So far we've managed to evade philosophical questions about mathematical objects. These are best faced head-on once, and not worried about later. Today we'll do just that.

ACTIVITY: Philosophical questions.

Here are some questions about some of the counterintuitive ideas we've seen so far in this course:

1. We saw that all mathematical objects– real numbers, geometric objects, functions– can be thought of as complicated sets. Is this actually "true"? Or are these just to be thought of as encodings of the objects, which already exist?
2. Do our considerations about infinity have any bearing on the real world? For example, is the set of objects in the universe countable, uncountable, or does it not make sense to ask?
3. The Banach-Tarski paradox shows that a sphere can be disassembled into 5 pieces which can be re-assembled into two copies of the same sphere. These pieces are infinitely detailed, so cannot be physical. Does this diminish the paradox at all?
4. There are some statements, like the continuum hypothesis, which cannot be proven or disproven from the commonly accepted axioms of mathematics. Does it make sense to ask whether these statements are "true" or "false"?

For each of the above ideas, write down a few sentences about your thoughts on the question.

A number of schools of thought emerged during the foundational crisis which have answers to these questions. Three of the most prominent are *Platonism*, *Formalism*, and *Intuitionism*.
Platonism asserts that mathematical objects exist independently of the human mind. A Platonist would answer the questions above as follows:

- Set theory should be thought of as an encoding of pre-existing mathematical objects, and axiomatic foundations are merely imperfect models of mathematical objects.
- The real world is distinct from the mathematical world, and so our considerations about infinity have no bearing on the real world. Questions about the cardinality of real-world sets only make sense insofar as we model them by objects in the mathematical world.
- Banach-Tarski is not diminished by the non-physical nature of the pieces of the sphere, since it is not a physical object.
- The continuum hypothesis, a mathematical statement, must be either true or false. Its independence from ZFC is a defect of the axiomatic system, not a defect of the statement itself.

Formalism asserts that mathematics is a game of symbols, and the only important thing is the formal rules of the game. A Formalist would answer the questions above as follows:

- If we model mathematical objects as sets, then they really are sets. There are no platonic mathematical objects.
- Since mathematical objects are purely formal, they have no bearing on the real world.
- Banach-Tarski is not diminished by the non-physical nature of the pieces of the sphere, since it is a purely formal argument.
- The continuum hypothesis is independent of ZFC; there is no definition of "true" or "false" for mathematical statements without reference to a model.

Intuitionism asserts that mathematical objects are created by the human mind through intuition. An Intuitionist would answer the questions above as follows:

- Mathematical objects are created by the human mind through intuition. There are no platonic mathematical objects, but the formal symbol-shuffling is not the same as the intuitive understanding of the objects.
- As a product of human intuition, mathematical arguments do have a bearing on the real world. For instance, if infinite sets cannot be constructed in practice, they should not be considered as actual mathematical objects.
- Since nonconstructive arguments are required to build the pieces of the sphere in Banach-Tarski, it is not a valid argument. The non-physical nature of the pieces is inherently linked to the non-constructive nature of the argument.
- The continuum hypothesis is essentially meaningless in the first place, since it concerns highly non-constructive objects.

Where do you fall? _____

Day 14: 28 October

Today: Incompleteness I.

Today begins our two-part discussion of the incompleteness theorems. It will use everything we've learned so far–models, axiomatic systems, computability, and more.
We'll start with the following paradoxes, which will lead us to the incompleteness theorems:

ACTIVITY: The liar paradox and variants.

For each of the following statements, determine whether it is true or false, and whether it is provable.

1. This statement is false.
2. This statement is not provable.

The full statement of Gödel's first incompleteness theorem is as follows:

Theorem (Gödel's first incompleteness theorem)**.** *Any consistent, computably axiomatizable theory which is strong enough to represent basic arithmetic has a statement which is true but not provable from the axioms.*

We should talk through the statement of the theorem in detail:

- A theory is *consistent* if it is not possible to prove a contradiction from the axioms.
- A theory is *computably axiomatizable* if there is a program which can list all of the axioms of the theory.
- A theory is *strong enough to represent basic arithmetic* if it can represent the natural numbers and the basic operations of arithmetic.
- A statement is *true* if it is true in all models of the theory.
- A statement is *provable* if there is a proof of the statement from the axioms.

The theorem states that there is a statement which is true but not provable from the axioms. On its face, the statement will look like "There does not exist a natural number with property P." But the property P will be chosen in such a way that the existence of such a number is equivalent to the provability of the statement itself.
The first big idea of the proof is to encode formulas as numbers, so that we can talk about the properties of formulas as properties of numbers. There's lots of ways to do this, called *Gödel numbering*. We'll use the following one:

(1) First every symbol in the first-order theory of arithmetic gets its own number:

symbol	number
0	1
+	2
$\times$	3
=	4
(	5
)	6
logical symbols ($\forall$, $\exists$, $\sim$, $\rightarrow$, $\wedge$, $\vee$)	7,8,9,10,11,12
variables (x, y, z, ...)	13, 14, 15, ...

(2) Next, we use this table to turn a formula into a sequence of numbers: for example, the formula 0=0 becomes $(1, 4, 1)$.

(3) Last, we use prime factorizations to turn this sequence of numbers into a single number:

$$(1,4,1) \to 2^1 \times 3^4 \times 5^1 = 810.$$

So the *Gödel number* of the formula `0=0` is 810. We write this as

$$\#(\texttt{0=0}) = 810.$$

The important property of Gödel numbering is that the translations between formulas and their Gödel numbers can be done computably in either direction. That is, we can write a program which converts a formula to its number, and vice versa.
Once we can think of numbers as representing formulas, we can use formulas to talk about other formulas, since our formulas are about arithmetical properties of numbers. For example, consider the property

"φ does not contain the symbol $+$."

On its face, this is not a property of numbers, but of formulas. But consider the property

"n is the Gödel number of φ, and n is not divisible by 3."

This is now an arithmetical property of the number n, but it is true if and only if φ does not contain the symbol $+$. That is, the *number property*

$$P(x) : x \text{ is not divisible by } 3$$

corresponds to the *formula property*

$$\mathcal{P}(\varphi) : \varphi \text{ does not contain } \texttt{+}.$$

This deserves emphasis: we have a correspondence

$$\Big\{\text{numbers}\Big\} \xleftrightarrow{\text{Gödel numbering}} \Big\{\text{formulas}\Big\}$$

which we can use to turn statements about formulas into statements about numbers:

$$\Big\{\text{number properties}\Big\} \longleftrightarrow \Big\{\text{formula properties}\Big\}$$

So if our formulas can talk about numbers, they can talk about formulas as well!
Next time, we'll use this to amazing fact to finish the proof. ———————————————

Day 15: 30 October

Today: Incompleteness II.

Last time, we used the technique of *Gödel numbering* to turn formulas into numbers and vice versa. This let us turn certain formula properties into number properties: If $\mathcal{P}(\varphi)$ is a formula property, then the corresponding number property states:

"the formula with number n has property $\mathcal{P}$."

A very natural question is: which formula properties can be translated in this way? It turns out that lots of properties can! But the only one we're worried about is provability. To represent provability, we have to extend our numbering system to allow not just formulas, but lists of formulas. This isn't too bad; let's just say that different formulas are separated by double arrows, like

$$0 = 0 \to\to \forall x \exists y (x + x = y) \to\to \cdots$$

Notice that some lists of formulas represent valid proofs, while others don't. And we can use the fact that our theory is computably axiomatizable to write down an arithmetical statement which verifies that a list of formulas is a valid proof!

If that's confusing, don't worry too much about it! The point is that the statement

$$P(n) = \text{"}n \text{ is the number of a proof of } \varphi\text{"}$$

can be written down as a purely arithmetical property of the number n; and thus the formula $\exists n P(n)$ is a purely arithmetical sentence about natural numbers, which nevertheless is true if and only if the formula φ is provable.

Now, setting provability aside for a moment, we consider the following: what happens if we have a formula $\varphi(x)$, and we plug in $\#\varphi$ itself for x?

Well, if we write

$$\varphi(x) \leftrightarrow x \text{ has property } P,$$

then it must be that

$$\varphi(\#\varphi) \leftrightarrow \#\varphi \text{ has property } P.$$

So we get a sentence stating that "$\#\varphi$ has property P". Call this new statement φ^*. Notice that the transformation $\varphi \mapsto \varphi^*$ is straightforward– just plug the number of φ into itself.

Now, we declare $\mathcal{P}$ to be the formula property that holds of a formula $\psi(x)$ if and only if the starred version ψ^* is *not* provable. We saw that provability is representable as a number property, so there is some corresponding number property P such that a number n has property P if and only if it is the number of a formula that has property $\mathcal{P}$. We let $\sigma_P(x)$ be the statement expressing that x has property P, and let $G = \sigma_P^*$. Then G holds if and only if σ_P has property P. But this holds if and only if σ_P^* is not provable, i.e., if and only if G is not provable! So G says of itself that it is not provable. As we saw on Day 14, this means that G must be true and not provable. And this finishes the proof!

What happened here? The main idea is that arithmetic is a powerful enough language that any system capable of expressing arithmetical statements is also capable of talking about formulas, using Gödel numbering. And its ability to talk about formulas means it can talk about provability within itself, and thus express the statement "this sentence is not provable". This statement is true, but cannot be proved.

When Gödel proved his results, many mathematicians still believed that a complete, consistent, computably axiomatizable theory of mathematics was within reach. But this result destroys any hope of writing down a list of axioms which proves or disproves every mathematical statement.

There is much, much more to say, but we'll stop here.