
# Class 36: Proofs about Unprovability

David Evans
University of Virginia cs1120

## Story So Far

- Much of the course so far:
  - Getting comfortable with recursive definitions
  - Learning to write programs that do (almost) anything (PS1-4)
  - Learning more expressive ways of programming (PS5-7)
- Starting today and much of the rest of the course:
  - Getting ***un***-comfortable with recursive definitions
  - Understanding why there are some things **no program can do**!

## Computer Science/Mathematics

Monday

- Computer Science (Imperative Knowledge)
  - Are there (well-defined) problems that cannot be solved by *any* procedure?

Today

- Mathematics (Declarative Knowledge)
  - Are there true conjectures that cannot be the shown using *any* proof?

## Mechanical Reasoning

Aristotle (~350BC): *Organon*

Codify logical deduction with rules of inference (syllogisms)

Every $A$ is a $P$
$X$ is an $A$ — Premises
$X$ is a $P$ — Conclusion

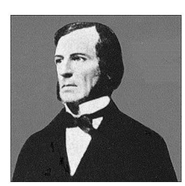
Every *human* is *mortal*.
*Gödel* is *human*.
*Gödel* is *mortal*.

## More Mechanical Reasoning

- Euclid (~300BC): *Elements*
  - We can reduce geometry to a few axioms and derive the rest by following rules
- Newton (1687): *Philosophiæ Naturalis Principia Mathematica*
  - We can reduce the motion of objects (including planets) to following axioms (laws) mechanically

## Mechanical Reasoning

1800s – mathematicians work on codifying "laws of reasoning"



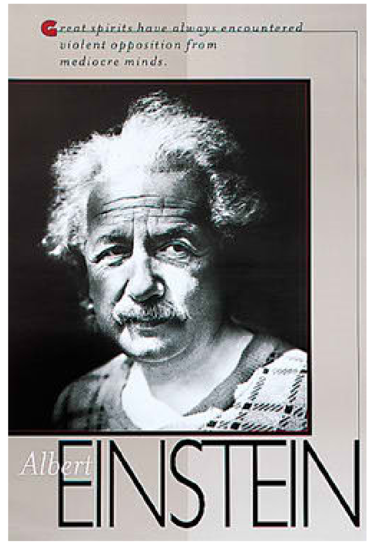
George Boole (1815-1864)
*Laws of Thought*

Augustus De Morgan (1806-1871)
De Morgan's laws
proof by induction

## Bertrand Russell (1872-1970)

- 1910-1913: *Principia Mathematica* (with Alfred Whitehead)
- 1918: Imprisoned for pacifism
- 1950: Nobel Prize in Literature
- 1955: Russell-Einstein Manifesto
- 1967: *War Crimes in Vietnam*

Note: this is the same Russell who wrote *In Praise of Idleness*!




When Einstein said, "Great spirits have always encountered violent opposition from mediocre minds." he was talking about Bertrand Russell.

All **true** statements about numbers

## Perfect Axiomatic System

Derives **all** true statements, and **no** false statements starting from a finite number of axioms and following mechanical inference rules.

## *Incomplete* Axiomatic System

incomplete

Derives **some, but not all true** statements, and **no false** statements starting from a finite number of axioms and following mechanical inference rules.

## *Inconsistent* Axiomatic System

Derives **all true** statements, **and some false** statements starting from a finite number of axioms and following mechanical inference rules.

**some** false statements

# *Principia Mathematica*

- Whitehead and Russell (1910– 1913)
  - Three Volumes, 2000 pages
- Attempted to axiomatize mathematical reasoning
  - Define mathematical entities (like numbers) using logic
  - Derive mathematical “truths” by following mechanical rules of inference
  - Claimed to be *complete* and *consistent*
    - All true theorems could be derived
    - No falsehoods could be derived

# Russell’s Paradox

Some sets are not members of themselves

e.g., set of all Jeffersonians

Some sets are members of themselves

e.g., set of all things that are non-Jeffersonian

*S* = the set of all sets that are not members of themselves

Is *S* a member of itself?

# Russell’s Paradox

- *S* = set of all sets that are not members of themselves
- Is *S* a member of itself?
  - If *S* **is** an element of *S*, then *S* **is** a member of itself and should **not** be in *S*.
  - If *S* **is not** an element of *S*, then *S* **is not** a member of itself, and **should** be in *S*.

# Ban Self-Reference?

- *Principia Mathematica* attempted to resolve this paragraph by banning self-reference
- Every set has a type
  - The lowest type of set can contain only “objects”, not “sets”
  - The next type of set can contain objects and sets of objects, but not sets of sets

# Russell’s Resolution (?)

$\text{Set} ::= \text{Set}_n$

$\text{Set}_0 ::= \{\ x \mid x$ is an $Object\ \}$

$\text{Set}_n ::= \{\ x \mid x$ is an $Object$ or a $Set_{\underline{n-1}}\ \}$

$S$: $\text{Set}_n$

Is $S$ a member of itself?

No, it is a $\text{Set}_n$ so, it can’t be a member of a $\text{Set}_n$

# Epimenides Paradox

Epidenides (a Cretan):

“All Cretans are liars.”

Equivalently:

“This statement is false.”

Russell’s types can help with the set paradox, but not with these.

## Gödel's Solution

All consistent axiomatic formulations of number theory include *undecidable* propositions.

*undecidable* – cannot be proven either true or false inside the system.

## Kurt Gödel

- Born 1906 in Brno (now Czech Republic, then Austria-Hungary)
- 1931: publishes *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* (*On Formally Undecidable Propositions of Principia Mathematica and Related Systems*)

1939: flees Vienna

Institute for Advanced Study, Princeton

Died in 1978 – convinced everything was poisoned and refused to eat

## Gödel's Theorem

In the *Principia Mathematica* system, there are statements that cannot be proven either true or false.

## Gödel's Theorem

In any interesting rigid system, there are statements that cannot be proven either true or false.

## Gödel's Theorem

All logical systems of any complexity are incomplete: there are statements that are *true* that cannot be proven within the system.

## Proof – General Idea

- Theorem: In the *Principia Mathematica* system, there are statements that cannot be proven either true or false.
- Proof: Find such a statement

## Gödel's Statement

*G*: This statement does not have any proof in the system of *Principia Mathematica*.

*G* is unprovable, but true!

## Gödel's Proof Idea

*G*: This statement does not have any proof in the system of *PM*.

If *G* is **provable**, PM would be **inconsistent**.

If *G* is **unprovable**, PM would be **incomplete**.

Thus, **PM cannot be complete and consistent!**

## Gödel's Statement

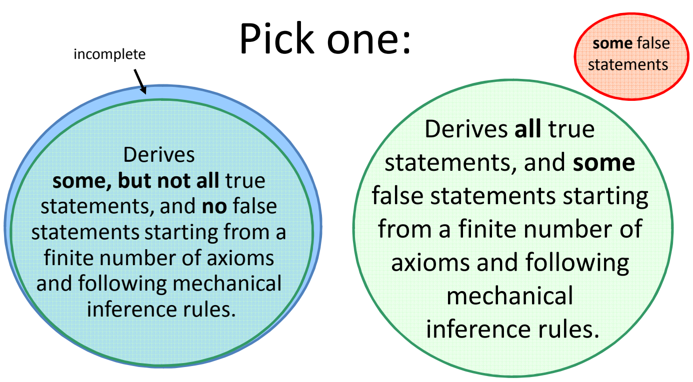
*G*: This statement does not have any proof in the system of *PM*.

Possibilities:

1. *G* is **true** $\Rightarrow$ *G* has no proof
   System is ***incomplete***

2. *G* is **false** $\Rightarrow$ *G* has a proof
   System is ***inconsistent***

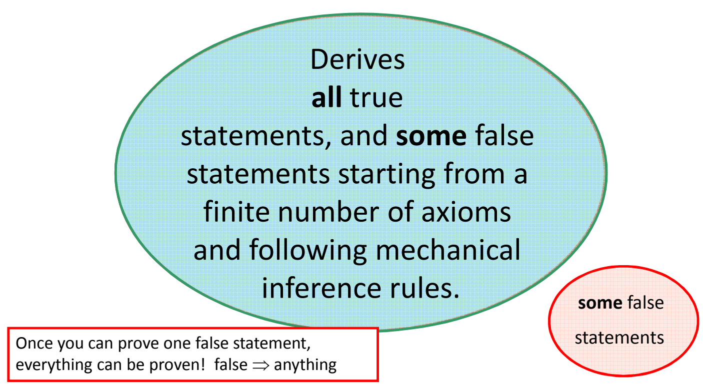
## Pick one:




*Incomplete* Axiomatic System

*Inconsistent* Axiomatic System

## *Inconsistent* Axiomatic System



## Finishing The Proof

- Turn $G$ into a statement in the *Principia Mathematica* system
- Is *PM* powerful enough to express $G$:

"This statement does not have any proof in the *PM* system."

?

## How to express "does not have any proof in the system of *PM*"

- What does "have a proof of $S$ in PM" mean?
  - There is a sequence of steps that follow the inference rules that starts with the initial axioms and ends with $S$
- What does it mean to "**not** have **any** proof of $S$ in PM"?
  - There is **no** sequence of steps that follow the inference rules that starts with the initial axioms and ends with $S$

## Can PM express unprovability?

- There is **no** sequence of steps that follows the inference rules that starts with the initial axioms and ends with $S$
- Sequence of steps:

$T_0, T_1, T_2, \ldots, T_N$

$T_0$ must be the axioms
$T_N$ must include $S$
Every step must follow from the previous using an inference rule

## Can we express "This statement"?

- Yes!
- If you don't believe me (and you shouldn't) read the TNT Chapter in *Gödel, Escher, Bach*

We can write every statement as a number, so we can turn "This statement does not have any proof in the system" into a number which can be written in PM.

## Gödel's Proof

$G$: This statement does not have any proof in the system of *PM*.

If $G$ is provable, PM would be inconsistent.

If $G$ is unprovable, PM would be incomplete.

PM can express $G$.

Thus, **PM cannot be complete and consistent!**

## Generalization

All logical systems of any complexity are incomplete:

there are statements that are *true* that cannot be proven within the system.

# Practical Implications

- Mathematicians will ***never*** be completely replaced by computers
  - There are mathematical truths that cannot be determined mechanically
  - We can write a program that automatically proves only true theorems about number theory, but if it *cannot* prove something we do not know whether or not it is a true theorem.

# What does it mean for an axiomatic system to be complete and consistent?

Derives **all** true statements, and **no** false statements starting from a finite number of axioms and following mechanical inference rules.

# What does it mean for an axiomatic system to be complete and consistent?

It means the axiomatic system is weak.

Indeed, it is *so* weak, it cannot express:
"This statement has no proof."

# Charge

- Monday
  - How to prove a problem has no solving procedure
- Wednesday, Friday: enjoy your Thanksgiving!

Exam 2 is due Monday