Class 23: Gödel’s Theorem

PS5

How are commercial databases different from what you implemented for PS5?

UVa’s Integrated Systems Project to convert all University information systems to use an Oracle database was originally budgeted for $58.2 Million (starting in 1999). Actual cost is likely to be $100 Million.

http://www.virginia.edu/isp/

Real Databases

- Atomic Transactions: a transaction may involve many modifications to database tables, but the changes should only happen if the whole transaction happens (e.g., don’t charge the credit card unless the order is sent to the shipping dept)
- Security: limit read/write access to tables, entries and fields
- Storage: need to efficiently store data on disk, provide backup mechanisms
- Scale: to support really big data tables, real databases do lots of clever things

How big are big databases?

- Microsoft TerraServer
  - Claimed biggest in 1998
  - Aerial photos of entire US (1 meter resolution)

You are here

Rotunda

AFT

Picture from 2 Apr 1994
Big Databases
- Microsoft TerraServer
  - 3.3 Terabytes (claimed biggest in 1998)
  - 1 Terabyte = $2^{40}$ Bytes ~ 1 Trillion Bytes
- Google Maps
  - Not so big? (but offers programming interface!)
- Wal-Mart
- Stanford Linear Accelerator (BaBar)
  - 500 Terabytes (30 KB per particle collision)

How much work?
- table-select is $\Theta(n)$ where $n$ is the number of entries in the table
- Would your table-select work for Wal-Mart?
- If 1M entry table takes 1s, how long would it take Wal-Mart to select from 285TB ~ 2 Trillion Entries?
  2 000 000s ~ 23 days

How do expensive databases perform so much faster?

PS6
Make an adventure game programming with objects

Many objects in our game have similar properties and behaviors, so we use inheritance.

PS6 Classes

PS6 Objects

Are there class hierarchies like this in the “real world” or just in fictional worlds like Charlottansville?
Microsoft Foundation Classes

CButton inherits from CWnd inherits from CObject
“A button is a kind of window is a kind of object”

Java 3D Class Hierarchy Diagram:

Not at all uncommon to have class hierarchies like this!

Story So Far

• Much of the course so far:
  – Getting comfortable with recursive definitions
  – Learning to write a program to do (almost) anything (PS1-4)
  – Learning more elegant ways of programming (PS5-6)
• This Week:
  – Getting uncomfortable with recursive definitions
  – Understanding why there are some things no one can write a program to do!

Computability

Decidable
All Problems

Computer Science/Mathematics

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

• Mathematics (Declarative Knowledge)
  – Are there true conjectures that cannot be shown using any proof?

Problem Classes if P ≠ NP:
(From Lecture 16)
Mechanical Reasoning

- Aristotle (~350BC): *Organon*
  - We can explain logical deduction with rules of inference (syllogisms)
  - Every B is A
  - C is B
  - \( \therefore \) C is A
  - *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): *Philosophiae Naturalis Principia Mathematica*
  - We can reduce the motion of objects (including planets) to following axioms (laws) mechanically

Late 1800s – many mathematicians working on codifying “laws of reasoning”
- George Boole, *Laws of Thought*
- Augustus De Morgan
- Whitehead and Russell

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

- 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.

**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
  - set of all Jeffersonians
- Some sets are members of themselves
  - 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 Resolution?**

Set ::= \( \text{Set}_n \)

Set_0 ::= \{ \ x \mid x \text{ is an } Object \} 

Set_n ::= \{ \ x \mid x \text{ is an } Object \text{ or a } \text{Set}_{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 this one.

Gödel’s Solution

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

(GB, p. 17)

*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 of number theory does not have any proof in the system of *Principia Mathematica*.

\( G \) is unprovable, but true!

Gödel’s Proof
\( G \): This statement of number theory does not have any proof in the system of \( PM \).
If \( G \) were provable, then \( PM \) would be inconsistent.
If \( G \) is unprovable, then \( PM \) would be incomplete.

\( PM \) cannot be complete and consistent!

Finishing The Proof
• Turn \( G \) into a statement in the *Principia Mathematica* system
• Is \( PM \) powerful enough to express “This statement of number theory does not have any proof in the system of \( PM \).”?

How to express “does not have any proof in the system of \( PM \)”
• What does it mean to have a proof of \( S \) in \( PM \)?
  – 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 follow the inference rules that starts with the initial axioms and ends with \( S \)
- Yes: (using Scheme-ified Gödel notation)
  \[
  \text{unprovable? } x = (\text{not } \text{provable? } x) \\
  \text{provable? } x = (\exists y \text{ proves } x y) \\
  \text{proves } x y = \\
  (\text{and valid-proof-steps } x) \\
  (\text{eq? (apply-proof } x \text{ initial-axioms } y))
  \]

Can we express “This statement of number theory”

- Yes!
  - That’s the point of the TNT Chapter in GEB
- We can write turn every statement into a number, so we can turn “This statement of number theory does not have any proof in the system of PM” into a number

Gödel’s Proof

\( G \): This statement of number theory does not have any proof in the system of PM.

If \( G \) were provable, then PM would be inconsistent.

If \( G \) is unprovable, then PM would be incomplete.

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 build a computer that will prove only true theorems about number theory, but if it cannot prove something we do not know that that is not a true theorem.

Charge

- Wednesday:
  - Does not being able to prove things mechanically have anything to do with not being able compute things?
  - What is the equivalent to the Gödel sentence for computation?
- Friday:
  - How to prove a problem has no solving procedure