

Great Theoretical Ideas In Computer Science
V. Adamchik CS 15-251 Fall 2006
Lecture 27 Apr. 26, 2006 Carnegie Mellon University

Gödel's Legacy: Proofs and Their Limitations



A Quick Recap

Turing showed that there must exist
undecidable problems.

The Halting Problem

$K = \{P \mid P(P) \text{ halts} \}$

Is there a program HALT such that:

HALT(P) = yes, if $P \in K$
HALT(P) = no, if $P \notin K$

HALT decides whether or not any given
program is in K.

Alan Turing (1912-1954)

There is no program to
solve the halting
problem

In other words, there is
no algorithm for
deciding whether or not
a program ever halts.



Introduction

By the XX century there had been
established a few formal systems
(based on axioms) from which it seemed
reasonable that all theorems could be
derived by applying the rules of logic.

Introduction

Peano arithmetic

Zermelo-Fraenkel set theory

Euclidean geometry

Introduction

Hilbert had proposed a project which, if successful, would have led to the complete automation of mathematics.



Hilbert

Introduction

Hilbert thought it would be possible to develop an algorithm which, when applied to any statement, would completely automatically determine its truth.

Introduction

Hilbert:

The rules should be so clear, that if somebody gives you what they claim is a proof, there is a mechanical procedure that will check whether the proof is correct or not.

Introduction

Mathematics would be reduced to nothing more than calculation.

Introduction

Gödel's Incompleteness Theorem showed that Hilbert's plan was impossible

Gödel's Legacy

"My attempt to understand Gödel's proof took over my life"

Gregory Chaitin

Gödel's theorem

Let's take a look again at the liar paradox:

"This statement is false!"

"This statement is false!"

The first thing that Gödel does is to change it to

"This statement is unprovable!"

Gödel's theorem

What do we mean by "unprovable"?

Or what do we mean by "provable"?

What do we mean by "provable"?

You have to say very precisely what the axioms and methods of reasoning you have in mind.

This proof-checking algorithm is the heart of a Formal Axiomatic System.

Gödel's theorem

This statement is false

This statement is unprovable

This statement is unprovable_{FAS}

Gödel's theorem

This statement is unprovable_{FAS}

The particular formal axiomatic system that Gödel was interested in dealt with the positive integers, addition and multiplication - the axioms of Peano Arithmetic.

This statement is unprovable_{FAS}

There are two possibilities: either it's provable or it's unprovable.

1. If it's unprovable then it's true statement. Therefore, our FAS is not complete.

This statement is unprovable_{FAS}

There are two possibilities: either it's provable or it's unprovable.

2. If it's provable then we prove something that is false.

Gödel's incompleteness

Gödel's incompleteness result is that if you assume that only true theorems are provable, then

This statement is unprovable_{FAS} is an example of a statement that is true but unprovable in the theory.

Gödel's incompleteness



But wait a second, how can a statement deny that it is provable?

Gödel's incompleteness

Gödel cleverly converts

"This statement is unprovable_{FAS}" into an arithmetical statement.

Gödel number

The trick is to replace each symbol in the proposition, including numerals, by a different string of digits.

If we represent "1" by 01, "2" by "02", "+" by 10 and "=" by "11", then the Gödel number of

"1+1=2" is 0110011102.

Gödel's incompleteness

Gödel showed that every syntactically correct proposition in Peano Arithmetic can be represented by a unique integer, which is called the Gödel number.

In particular, any proof in PA corresponds to a number.

Peano axioms

1. Every natural number n has a successor, denoted by $s(n)$.
2. Zero is not the successor
3. Distinct natural numbers have distinct successors: $s(n)=s(m) \Rightarrow n=m$
4. $0*n = 0$
5. $n*s(m) = n + n*m$
6. If a property holds for 0, and holds for the successor of every natural number for which it holds, then the property holds for all natural numbers.

Peano Arithmetic

The theory obtained by using the above axioms along with the apparatus of first order predicate calculus is called first order Peano arithmetic.

First Order Predicate Calculus

A predicate calculus consists of

1. formation rules (i.e. recursive definitions for forming well-formed formulas).
2. transformation rules (i.e. a scheme for deriving theorems, modus ponens);
3. a set of logical axioms

Modus Ponens

$$[P \text{ and } P \rightarrow Q] \rightarrow Q$$

Everyone taking 251 knows where Aha comes from.
John takes 251.
Therefore, John knows where Aha comes from.

Gödel's incompleteness

From here, Gödel showed that, either the system is inconsistent, or there are true propositions which can't be reached from the axioms.

Gödel's incompleteness

There is such function G that
 $G(m, n) = 0$, if n is the Gödel number of
the proof of the statement with Gödel
number m .

Gödel's incompleteness

Consider a new statement

$$S(m) = "\forall n, G(m, n) \neq 0"$$

Let its Gödel number be i .
Consider $S(i)$. Is it provable?

$$S(i) = "\forall n, G(i, n) \neq 0"$$

Suppose $S(i)$ is provable. Then that
proof will have Gödel number j .

What can you say about

$$G(i, j)$$

Gödel's incompleteness

$$G(i, j) = 0$$

which contradicts to

$$S(m) = "\forall n, G(m, n) \neq 0"$$

So, $S(i)$ cannot have a proof.



Peano Arithmetic is sound for the
truth concept of (first order)
number facts about natural numbers.

In other words, it means that we
can't prove anything false for the
truth concept.

$$S(i) = "\forall n, G(i, n) \neq 0"$$

So, $S(i)$ cannot have a proof.

But, $S(i)$ is true statement !



A logic may be sound but it still might not be "complete".

A logic is complete for a truth concept if it can prove every statement that is True

Peano Arithmetic is sound, but it is not complete.



Incomplete system

The Elements of Euclid are sound and complete for (Euclidean) geometry.

If we drop the parallel postulate, we get an incomplete system.

Gödel's incompleteness theorem

If a proof system for arithmetic is sound (meaning that only true formulas are provable) then there must be a true formula that is not provable.



Gödel's incompleteness theorem

You can add *all true statements* about the natural numbers to your list of axioms.

Given a random statement, there will be no way to know if it is an axiom of your system.

If I give you a proof, in general there will be no way for you to check if that proof is valid.



No fixed set of assumptions can provide a complete foundation for mathematical proof.



So what is mathematics?



So what is mathematics?

We can still have rigorous, precise axioms that we agree to use in our reasoning (like the Peano Axioms, or axioms for Set Theory). We just can't hope for them to be complete.

Most working mathematicians never hit these points of uncertainty in their work, but it does happen!

Goldbach's Conjecture

every even integer number > 2 can be expressed as the sum of two primes.

Is it true?
Is it provable?

Final Remark

Gödel's incompleteness theorem is not a good excuse for being unable to find a proof in HWs and/or exams.