CS 4510

Gödel Incompleteness

Name: Abrahim Ladha

1.1 Introduction

What is the difference between a theorem and a corollary? a lemma? What is a proof? Take a minute to think about your internal, colloquial answer.

To me, its about scope. The theorem is the main focus. A lemma, is a tiny theorem used to prove a more important theorem. A corollary is a tiny theorem which can easily follow after the proof of a main theorem. Either way, there is an ordering, a flow of implication. Given a theorem, it follows from other theorems, which follow from others. If you try and walk backwards up this giant tree of knowledge, this directed graph, you should reach the roots; a set of statements with no proofs. We denote this set, which we do not prove, as the axioms.

Definition 1.1 (Axioms) *An axiom*[1] *is a logical statement assumed to be true. An axiomatic system is a set of axioms, with some rules of deduction to derive truths, within the axiomatic system.*

A thereom is then a true statement which is not an axiom. A proof can then be well defined, as a sequence of deductions from an axiomatic system, to a theorem. The rules of deduction are themselves axioms. An an example, consider some of the elementary axioms of propositional logic.

- (Law of Modus Ponens) $((p \implies q) \land p) \implies q$
- (Law of Excluded Middle) $(p \lor \neg p)$
- (Law of Double Negation) $\neg\neg p \iff p$
- (DeMorgans Law) $\neg(p \land q) \iff (\neg p \lor \neg q)$

These are just some. A proof is then a sequence of applications of axioms.

Definition 1.2 (Independence) *We say an axiomatic system is independent if each axiom cannot be deduced from the others*

You may think of this similar to linearly independent vectors. Given a set of axioms, there should exist no proof of one of the axioms following the others. You may recall the axioms of real numbers. The encouragement is that the axioms are statements so simple, that they cannot be proved. Like associativity of addition, $a+(b+c)=(a+b)+c$. The difference between an axiom and a theorem, is that a theorem has a proof from the axioms.

Definition 1.3 (Consistency) *We say an axiomatic system is consistent if any there does not exist a proof of p and $\neg p$ for p any axiom or theorem in the system.*

Seems reasonable that a good axiomatic system should be consistent. If there exists a proof of p and $\neg p$, then p and $\neg p$ are both true, so p is both true and false. It should be free of contradictions.

[1] or postulate

1.2 History

One of the first example of axiomatic thinking was Euclids Elements. Its such a famous book it has remained in print continuously for 2300 years, second only to the bible. It is a series of twelve books, each just axioms and definitions about what we now call euclidean geometry.

The first five postulates make up the first book of Euclid. He also defined points, lines, and surfaces. The first four axioms are as follows:

1. *To draw a straight line from any point to any point* (between any two points, you can always draw a straight line)
2. *To produce a finite straight line continuously in a straight line* (You can always make a line segment longer. We are on an infinite plane, $\mathbb{R}^2$)
3. *To describe a circle with any center and distance* (Given two points, you can make one the center, and one on the edge, with the radius the line segment between the two)
4. *All right angles are equal to each other*

Euclid's fifth postulate is originally[2] stated as follows

5. *That, if a straight line falling on two straight lines make the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.*

This is attempting to define parallel lines. Because it is a messy, and ambiguous definition, the reader feels invited to bring their own connotations and assumptions. The bandage tried throughout history was to deduce the fifth postulate from the previous four. This would imply you could take it as a theorem, instead of an axiom, and everything would be fine. This was first attempted by Ptolemy in the first century AD. In 1840, Lobachevsky[3] was one of the first to notice alternative systems of geometry which would satisfy the axioms. The fifth postulate was later repaired, and restated as follows.

5. *Given a line, and a point not on that line, there exists* ***exactly one*** *line through the point parallel to the line*

If you assume there exists more than one parallel lines through a point, you get hyperbolic (or Lobachevskian) geometry. If you assume no lines are parallel, then you get spherical geometry. If you assume exactly one, then you get Euclidean geometry!

The contribution by Lobachevsky that we care about is that he showed the fifth postulate cannot be proved from the first four.

Definition 1.4 (Completeness) *We say an axiomatic system is complete if every statement, or its negation is provable from the axioms. An axiomatic system is incomplete if there exists a statement where neither it, nor its negation are provable from the axioms*

Continuing our analogy of linear algebra, you may think a complete axiomatic system like a spanning basis of a vector space. Every statement, or its negation is provable from a complete system, like how every vector is a linear combination of only basis elements. Lobachevsky said the first four axioms are incomplete. In fact, the first five axioms are incomplete.

[2] Actually, I suppose it was originally in ancient greek

[3] Here is a song about him plagiarizing: https://www.youtube.com/watch?v=UQHaGhC7C2E

1.3 Principia Mathematica & ZFC

The logicist's thesis is that the mathematical theorems are a proper subset of the theorems of logic; Every mathematical proof has a representation as a deductive logical proof. During the early 20th century, there was work to find an axiomatic system which could formalize all of mathematics. Mathematicians began to notice that you could define a lot from a small set of assumed notions. Russell and Whitehead, among others spent many years writing Principia Mathematica, six volumes attempting to construct this. Much of the time was spent trying to prove completeness of PM, and they got very close.

ZFC[4] is what we still use today as the axioms for set theory. Set theory has been very kind to mathematics, as you may know. We can formalize anything as sets, graphs are sets, decision problems are languages, and so on. We define[5] the integers recursively as $0 = \emptyset, i + 1 = \emptyset \cup \{i\}$.

1.4 Setup

Definition 1.5 *A logical statement is a well formed string over* $\forall, \exists, (,), \vee, \wedge, \neg, \implies$ [6]*, and variables, we denote by letters.*

Definition 1.6 (Gödel Numbering) *A Gödel numbering* Γ *is a bijection* $\Sigma^* \to \mathbb{N}$.

Each logical statement can be interpreted as a string. All well-formed statements are then a subset of Σ^*. For each symbol, you assign an integer value. For example, let our table be:

x	$\Gamma(x)$
0	1
S	3
$\neg$	5
$\vee$	7
$\forall$	9
(	11
)	13

Notice we do not need all symbols. Recall deMorgans laws: $\exists = \neg\forall$, and $\neg\vee = \wedge$. For variables, we will assign primes > 13

x	$\Gamma(x)$
x	17
y	19
...	...

We can compute $\Gamma(x)$ by first interpretting x as a string of symbols, and converting to an ordered set of numbers, from the table. Then for our ordered set, we compute them as prime powers. Let $x = x_1...x_n$. Then let the number for symbol x_i be $T(x_i)$. We define

$$\Gamma(x) = \prod_{i=1}^{n} p_i^{T(x_i)} \tag{1.1}$$

[4]Stands for ZF + C, which stands for the Zermelo-Fraenkel axioms with the axiom of choice

[5]Called the Von-Neumann ordinals

[6]Implication is actually not nessessary, just useful. Recall $p \implies q \iff \neg p \vee q$

Where p_i is the i'th prime. Lets do an example. Consider the law of excluded middle. As a logical statement it says every statement is either true or not true[7].

$$\forall x(x \vee \neg x) \quad (1.2)$$

$$\forall, x, (, x, \vee, \neg, x,) \quad (1.3)$$

$$9, 17, 11, 17, 7, 5, 17, 13 \quad (1.4)$$

$$2^9, 3^{17}, 5^{11}, 7^{17}, 11^7, 13^5, 17^{17}, 19^{13} \quad (1.5)$$

$$2^9 \cdot 3^{17} \cdot 5^{11} \cdot 7^{17} \cdot 11^7 \cdot 13^5 \cdot 17^{17} \cdot 19^{13} \quad (1.6)$$

$$189043632009771568293834434179998048570239668862186531325541111262918202225 \cdot 10^9 \quad (1.7)$$

Recall that we gave Turing machines encodings, to allow them to talk about themselves. Turing originally did not use encodings, but literally Gödel numberings. Back then, this was more of a new idea, to encode objects as numbers, and then to talk about them as data. Now we use computers all the time, which has images, sounds, and more encoded as numbers, so this is more natural to us. The proof Γ is bijective directly comes from the fundamental theorem of arithmetic. We can now use the Gödel numbering to allow our system to talk about itself. If some $p_i^j | \Gamma(x)$, this can tell us something about x.

Definition 1.7 $\forall x, y \in \mathbb{N}, xDy \iff \Gamma^{-1}(x)$ *is a proof of* $\Gamma^{-1}(y)$.

This relation[8] is actually primitive recursive! I won't demonstrate it. The proof is not hard, but it is very very long, involving us to prove 40+ other primitive recursive relations. It builds upon the fact we can test certain properties of a statement depending upon prime divisors of it's Gödel numbering. We will show one of the relations, as it will be useful to us.

Definition 1.8 *Let* $xS(v, y)$ *denote the relation where with* v *a free variable, we replace with string* y.

Here S is for substitute. In order to determine a truth value of a statement, we must quantify every variable, and this allows us to evaluate statements. I claim this relation is also primitive recursive, without proof.

1.5 The Incompleteness Theorems

Theorem 1.9 (Gödel's First Incompleteness Theorem) *Any consistent axiomatic system with sufficient arithmetic is incomplete*

What exactly "sufficient arithmetic" means is complex. For us, lets suppose that it means all primitive recursive functions are definable within the system. Consider the statement

$$\neg\exists x(xDy) \quad (1.8)$$

In human words, y is not provable. There is no x such that $\Gamma^{-1}(x)$ is a proof of $\Gamma^{-1}(y)$. Now consider the statement with one free variable as

[7] The faction of people which deny this are called the intuitionists, but it seems pretty intuitive to me

[8] We have only talked about PR functions, not relations, but they are the same. We save a relation is PR if its characteristic function is PR. Recall that a relation is just a subset $R \subseteq \mathbb{N} \times \mathbb{N}$. The characteristic function of a set is $\chi_R = \{1 \text{ if } (x, y) \in R; 0 \text{ if } (x, y) \notin R\}$

$$p(y) = \neg\exists x(xD(yS(19, y))) \tag{1.9}$$

We substitute the variable y, with the literal value y. What is $p(\Gamma(p))$? Since our system is complete, and this statement has no free variables, it should either be assigned a value of true or false. Lets inspect

$$p(y) = \neg\exists x(xD(yS(19, y))) \tag{1.10}$$
$$p(\Gamma(p)) = \neg\exists x(xD(\Gamma(p)S(19, \Gamma(p)))) \tag{1.11}$$
$$p(\Gamma(p)) = \neg\exists x(xD(p(\Gamma(p)))) \tag{1.12}$$

What $p(\Gamma(p))$ is, is a valid logical statement within the system, which states "I am not provable in the system". Wow! It has no free variables, so must have some truth value.

- Suppose $p(\Gamma(p))$ is true, there exists a proof of it. Then we have a statement which is not provable from the axioms, so the system is incomplete.
- Suppose $p(\Gamma(p))$ is false, then there must exist a proof of $\neg p(\Gamma(p))$. This implies

  $$\neg p(\Gamma(p)) = \neg\neg\exists x(xDp(\Gamma(p))) = \exists x(xDp(\Gamma(p))) \tag{1.13}$$

  This says there exists a proof of $p(\Gamma(p))$. So if $\neg p(\Gamma(p)) \wedge p(\Gamma(p))$, then the system was never consistent, a contradiction.

You might try and act cute. If you try to say "Well sure, I can't prove $p(\Gamma(p))$, so lets just take it as an axiom, so I don't have to prove it!". The beauty in Gödels proof is that I can then always construct another statement like $p(\Gamma(p))$. Adding in axioms adds in more unprovable statements.

Theorem 1.10 (Gödel's Second Incompleteness Theorem) *Any axiomatic system is incapable of proving its own consistency.*

Proof: Gödel's first incompleteness theorem states if an axiomatic system is consistent, then it is incomplete. If C is the logical statement claiming the consistency of the system, and $p(\Gamma(p))$ is the statement claiming it cannot be proven, we can represent this as $C \implies p(\Gamma(p))$. If C is provable, then it must be true that $p(\Gamma(p))$ is. But we know it cannot be! A contradiction. ■

1.6 Some Remarks

Apply this to Principia Mathematica. The first theorem says that PM was an exercise in futility. For any axiomatic system, you can always construct a statement which cannot be proven in the system. There was no point trying to formalize all of mathematics. The second theorem says if PM was consistent, then you cannot prove its own consistency. So trying to prove the consistency of PM was also an exercise of futility.

Gödel attended a conference in 1930 to present the result. On the first day, David Hillbert gave his retirement speech, ending with the passion that there cannot exist an unsolvable problem. On the third day, Gödel presented his result[9]. Imagine being Whitehead or Russell or Ackermann, or Hillbert. A young guy, 23, churns out a simple paper showing part of your life work was completely

[9] lmfao get owned formalists.

wasted. These men all had a gut feeling, about the way mathematics should work, and operated trying to prove it. Perhaps if they had stopped to consider the opposite, to ignore their gut, they might have saved themselves some time. This is a more common fate than you might imagine. Mathematician's can spend years in futile trying to prove a theorem, only to prove the negation in an afternoon.

You may notice a certain semblance to the proof by Turing[10] of the undecidability of the halting problem. They are related, and it is no secret Turing was inspired by Gödel's proof here. First, some universality is assumed to the contrary. That there exists a consistent complete axiomatic system, or a Turing machine to determine halting. Second, a contradiction is constructed, which is self-referential in nature. To say something about the system is to say something contradictory about itself.

Gödel incompleteness does not say you can never proof consistency of a system, just that if the system is strong enough to contain arithmetic, you cannot prove it from within the system. There are small toy models you can make, and prove its consistency stronger principles. Gödel had earlier proved the completeness of weaker systems, like first order logic.

Gödel incompleteness is a huge result, but it has not been that influential to broader mathematics. Sure, logic is foundational, and very important, but much of mathematics has been abstracted very far. When was the last time you knew which axiom of ZFC you were calling in a simple proof? Even though there exist undecidable problems, and unprovable statements, most of them are meta. There are very few examples of undecidable problems not related to logic itself.

The next biggest impossibility result would be the independence of the continuum hypothesis. CH states there is no set larger than a countable set, but smaller than an uncountable one.

$$\neg\exists x(\aleph_0 < x < \aleph_1); \qquad \aleph_1 = 2^{\aleph_0} \tag{1.14}$$

Paul Cohen, building off of work by Gödel, proved that CH was independent of ZFC. You can take either $\neg CH$, or CH as an axiom, since you cannot prove it, or its negation, within ZFC.

1.7 Summary

We can greatly shorten the proof of the first incompleteness theorem if you can bring some assumptions. Suppose we are in a complete and consistent axiomatic system with arithmetic, and lets suppose the logical statement "this statement is not provable from the axioms" can be well defined, in our system. Then either its true, and we have an unprovable statement, or if its false, then we are not consistent.

1.8 Problems

Pick three of four

1. Every logical statement has a unique Gödel numbering, but this is a syntatic property, not a semantic one. $(x \iff y) \not\Longrightarrow (\Gamma(x) = \Gamma(y))$, but $(\Gamma(x) = \Gamma(y)) \implies (x \iff y)$.
    - Construct two logically equivalent statements with different Gödel numberings.
    - Given a logical statement, construct an infinite family of equivalent logical statements, each with different Gödel numberings.

[10] Also Church, if you are familiar with his proof

2. Show that $xS(v, y)$ is computable by giving a Turing machine that computes it.

3. Show that the existence of undecidable problems implies a weak form of Godel's First Incompletness Theorem by proving the following: (ZFC is consistent and complete) $\rightarrow$ (HALT is decidable)"

4. Show that the set of unprovable statements is not Turing-recognizable.

Further Reading

[1] Jack Evoniuk. "Gödel's Incompleteness Theorems". In: (2020). URL: https://evoniuk.github.io/Godels-Incompleteness-Theorems/.

[2] Wikipedia contributors. *Original proof of Gödel's completeness theorem — Wikipedia, The Free Encyclopedia*. https://en.wikipedia.org/w/index.php?title=Original_proof_of_G%C3%B6del%27s_completeness_theorem&oldid=996654294. [Online; accessed 25-March-2021]. 2020.

[3] Thomas Little Heath et al. *The thirteen books of Euclid's Elements*. Courier Corporation, 1956.

[4] Kenneth Kunen. *Set theory an introduction to independence proofs*. Elsevier, 2014.