Foundations of Mathematics

Abraham Cadkra

Recall last time we had a lecture on pure mathematics, countability and set theory. The lecture before that was pseudo-philosophical on the Church-Turing Thesis. The lecture before that one was on engineering, programming and understanding the Turing machine. To keep the trend of not having one, todays lecture will be on history.

We begin of course, with the Greeks. we will go from 300BC to 1936. Around 300BC, Euclid compiled and wrote "The Elements", several treatises in geometry. One of the most influential texts of all time. It establishes mathematics as a deductive rather than empirical science.

Recall that a theorem is some statement proved from what? other theorems? not quite. There is some flow of implications in this giant tree of knowledge. ~~#~~ Follow back to eventually reach some root: The axioms. An axiom is a statement which needs no proof. It may be assumed to be true. It is usually so trivial to be anything but true. for example associativity of addition $(a+b)+c = a+(b+c)$.

Euclid defined his first five axioms as follows

I) ~~Between~~ any two points may be connected by a line segment

II) any line segment may be extended infinitely in both directions

III) for any point and radius there exists a circle

IV) All right angles are equal to one another

V) Given a line l and a point p not on that line. There exists exactly one line through p parallel to l.

A proof is an application of axioms using the "rules of deduction" (which are themselves axioms). These axioms (and the rest of the elements) are a <u>model</u> for what we now call Euclidean geometry. From the axioms you can prove things like: Every square has four equal right angles. The sum of the interior angles of a triangle is 180°. Many properties of bisecting ~~an~~ triangles and angles and circles and so on.

~~We have also spent milenia trying to~~ s Euclids elements have nothing to do with geometry. ~~At~~ its core, it is about rigorous and systematic thinking. A by product of the school of thought Euclid (and other Greeks) came from (Idealism?) Ideas are the supreme achievement of ~~the~~ human beings. They are a refined, pure, reflection of the capability of the human mind. The Real and Ideal certainly have a duality (maybe even better known by other names, theory and practice?). ~~I~~ This school of thought asserts that the world, the materiality, is shaped by something prior to it. To understand the material you only need to understand the non-material. Abraham Lincoln used the Elements to train as a lawyer. To truly under stand what "demonstrate" means.

Milenia was spent trying to refine the elements, show they were only as good and simple as necessary. ~~An axiom~~ A set of axioms is ~~complete~~ independent if no axiom can be proved from the others, like independence wrt a basis of a vector space. The fifth axiom took much attention as it was the first really unobvious one. Let A be the parallel postulate and EE the ~~rest of the~~ axioms. First people tried to see if you could prove it as a theorem. Could $EE - A \vdash A$?

here $\vdash$ ~~means~~ something is provable with respect to a set of axioms.

Another idea to understand the parallel postulate was to show that it was necessary. Try to prove that $EE - A + \neg A \vdash 0 = 1$ They tried to show that if you assumed the negation of the axiom, you reached a contradiction. a model with a false theorem is useless, as now all theorems are true. They discovered something insane. There was no contradiction, only alternate consistent models!

Given a line and a point not not that line there exists (≥ 1, $= 1$, < 1) lines through that point parallel to the line. if $= 1$ we have Euclidean geometry but

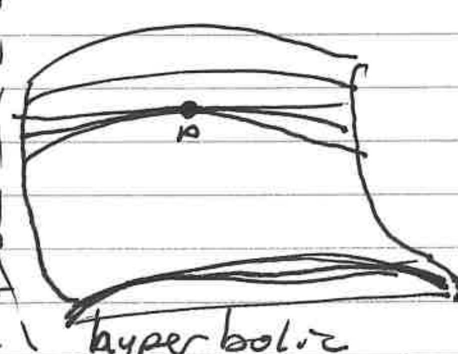
~~<1~~ 0

no nonintersecting

spherical

If we assume ≥ 1 we do not live on a flat world. we live on a pringle, or a saddle. There exist many "parallel" lines through p which do not intersect. Similarly if we assume

≥ 1



hyperbolic

that ~~<1~~ $= 0$, then no "parallel" lines exist, we are in a model of geometry embedded on a sphere (or ellipsoid). Note that these are <u>consistent</u> models. They cannot prove $0 = 1$ but all the rules are slightly different. for example in spherical geometry, a triangle has sum interior angles $= 180°$ $\Leftrightarrow$ it has area zero. Euclidean geometry is supposed to be "intuitive" but we discovered it was on all shaky foundations maybe the material world could follow these models? whos to say? how can we know? This spurred more serious concern and undertaking to the foundation of all of mathematics.

Logicomix pg 120.

A modern first attempt at formalizing mathematics was done by Gottlob Frege's "Begriffsschrift". It builds off of previous work by Leibniz and Aristotle's Organon. It identifies as "a formal language modeled on that of arithmetic, for pure thought". He also created many of our rules of deduction. For example $A \Rightarrow \neg\neg A$, $c = d \Rightarrow f(c) = f(d)$, $(A \wedge A \Rightarrow B) \Rightarrow B$ (modus ponens) and so on.

Bertrand Russell noticed the following issue, applied to many axiomatic systems. Suppose we have the following axioms (among others) for some theory of sets

$$1 \quad \forall x \, \forall y \left[\forall z \left(z \in x \Leftrightarrow z \in y \right) \Rightarrow x = y \right]$$

The axiom of extensionality simply defines equality of sets if they contain the same elements.

$$2 \quad \exists y \, \forall x \left[x \in y \Leftrightarrow \varphi(x) \right]$$

For any predicate φ, the axiom of unrestricted comprehension basically freely allows you to define any set you want. Like "let y be the set of primes, or horses or whatever". This generality is our fragility. Let $\varphi(x)$ be the sets which ~~don~~ do not contain themselves. Syntactically this is $\varphi(x) = x \notin x$. A perfectly valid predicate. By the axiom of unrestricted comprehension we see that

$$\exists y \, \forall x \left[x \in y \Leftrightarrow x \notin x \right]$$

Since its true $\forall x$, what happens for $x = y$?

$$y \in y \Longleftrightarrow y \notin y$$

A contradiction! See Logicomix 162 - 171

~~Also~~ Although this attack was devastating to Frege's work, it did not deter by much the resolve of the formalists. The formalists ~~are from~~ are a school of thought revolving around building Hilbert's program. They seek a secure, rigorous, and logical foundation in which to secure all of mathematics. Roughly with these ~~five~~ four goals.

- All math written in a precise formal language ~~...~~ manipulated according to well defined rules
- Completeness: all that is true is provable
- consistency You should provably be unable to obtain a contradiction
- Decidability There should be an algorithm to decide T/F in any statement.

The most significant effort in this regard was by Russell & Whitehead. They spent decades and thousands of pages to build up a "Theory of Types". They hoped to avoid self reference

unrestricted comprehension	restricted comprehension
$\{x \mid \varphi(x)\}$	$\{x \subseteq z \mid \varphi(x)\}$

by not allowing any statement to say anything about its own types. Also by ~~...~~ restricting comprehension, we avoid Russell's paradox. Is this system useful? Lets prove $1=1$. First let

$S(\emptyset) =$ $\emptyset$ exist by the axiom of restricted comprehension with some useless

$\{\emptyset\} =$ $\varphi(x) = \{x \in y \mid (x \in x) \wedge \neg(x \in x)\}$. Nothing satisfies it so we create $\emptyset$.

$\{\{\}\}$ Now let 0(zero) $:= \emptyset$. let $S(\omega) := \omega \cup \{\omega\}$. Let

$1: S(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$. We may now apply the axiom of ~~...~~

Is it true $\forall z [z \in \{\emptyset\} \Leftrightarrow z \in \{\emptyset\}]$? yes, then this implies that $1 = 1$. Supposedly to prove $1+1=2$ took PM 372 pages. This $1=1$ example is also

(or even ZF) from ZFC technically. Could PM serve as a suitable foundation? Free of issue? or somewhat incapable?

Gödel showed the futility of Russell and Whiteheads effort. We say an axiomatic system (AS) is:

complete If $\forall p$ $\exists$ a proof of p if its true, or a proof of $\neg p$ if its false. This asserts provable $\iff$ true

consisent $\forall p$ $\not\exists$ exist a proof of $p \wedge \neg p$. Every statement is exactly true or exactly false.

1st thm Godel show for any AS (including PM). It cannot be both consistent and complete. ~~In~~ Rephrasing: There does not exist ~~an~~ ~~a~~ complete and consisent axiomatic system with sufficient arithmetic. lets proceed with the proof

Let $Dem(p, r) = 1 \iff p$ is a proof of r
let

$$g = \neg \exists p \left[Dem(p, g) \right]$$

in human words, g says "I am not provable." or "There does not exist a proof of me." Notice the self reference. Since AS is complete, and consisent, one of g is provably true or provably false. We have two cases.

Case 1: g is provably true. Then g is true, and not provable. Now $\exists$ an unprovable statement, so we are incomplete.

Case 2 g is probably false. Then $\neg g$ is provably true.

$$\neg g = \cancel{\neg\neg} \exists p \left[Dem(p, r) \right]$$

so $\neg g \Rightarrow \exists$ a proof of $g \Rightarrow g$ is provably true. Then $[\neg g \wedge g]$ is provably true and we are inconsistent.

Not only does Gödel say that achieving a complete and consistent axiomatic system which is strong enough impossible but any system is incapable of proving its own consistency. Logically, for any axiomatic system AS

2nd thm $$AS \nvdash Con(AS)$$

The consistency of AS cannot be proven from within AS. Assume to the contrary $AS \vdash Con(AS)$, $\exists$ a proof of the consistency of AS from within AS. Let this proof be denoted as C. Since the proof of Gödel's first incompleteness theorem assumes the consistency of AS, we may replace this assumption by the proof C. Then we proceed and observe $C \Rightarrow g$, our diagonal sentence. Since we can construct g, then AS was not simultaneously consistent and complete, a contradiction $\square$

Not only were the formalists, Russell, Whitehead, Hilbert losers, they were double losers. The proof they spent decades searching for could never exist.

Russell
a loser
pg 130

Hilbert
a loser
pg 327

Gödel
not a loser
pg 326
just [illegible]

pg 112

takes a class foundations
Alan Turing ~~witnesses a lecture~~ on Gödel Incompleteness.
It also contains a description of then a large unsolved problem we will call "Hillberts decision problem" or "Entscheidungsproblem" - Give a procedure ~~algorithm~~ which takes as input a statement, and returns yes/no if its always true or always false. Hillbert genuinely believed there were no unsolvable problems. Turing was 22 when he solved it, maybe started it at 21, took a few months. First, we had to formalize the notion of computation, and to do so, he invented what we now call a Turing machine. He described the Church-Turing thesis to convince us that his definition was in fact universal.

Recall that a language $L \subseteq \Sigma^*$ is decidable if $\exists$ a Turing machine M such that

$$x \in L \iff M \text{ accepts } w$$
$$x \notin L \iff M \text{ rejects } w.$$

We can rephrase Hillberts decision problem as "~~show all languages are decidable~~ give a process to decide every language." Turing said no, and he did so in two ways.

First notice that the languages decidable by a Turing Machine are countable. I leave this as an exercise, since on HW3 you must prove $|\mathcal{L}(NFA)|$ is countable, and the argument is similar, maybe identical. His second observation is that the number of languages is uncountable. If $L \subseteq \Sigma^*$ then $\Rightarrow L \in \mathcal{P}(\Sigma^*)$ since $|\Sigma^*|$ is countable, $|\mathcal{P}(\Sigma^*)|$ is uncountable by Cantors theorem. There exists no surjection $\Sigma^* \to \mathcal{P}(\Sigma^*)$ so there must exist undecidable languages! infinitely many in fact. Most languages are undecidable using this simple nonconstructive counting proof.

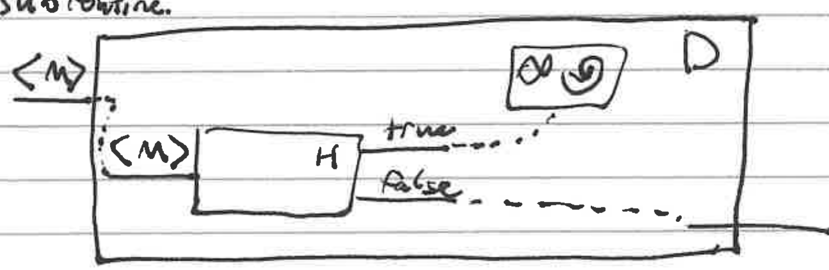
Now let us prove constructively that there exists real concrete unsolvable problems.

$$\text{HALT} = \{ \langle M, w \rangle \mid M \text{ halts on } w \}$$

HALT is a language of pairs of encodings of Turing machines and possible inputs, where $\langle M, w \rangle \in \text{HALT} \iff M$ halts on input w. We show that Halt is not decidable. This means there is no general algorithm to decide if a TM will halt on an input! An provably unsolvable problem!

Assume to the contrary that HALT is decidable. Then there exists a Turing machine $H(\langle M \rangle)$ on input $\langle M \rangle$ always says yes/no if $\langle M \rangle$ halts (ignore w for simplicity). We represent H like... an API or some IDE plugin or something, and build D around using calls to H, like H is its subroutine.

```
def D(M):
  ans = H(M):
  if ans
    loop
  else
    return
```



Recall since H is a decider, H halts on all inputs. What is D on input D? $D(\langle D \rangle)$? two cases.

$D(\langle D \rangle)$ halts $\iff$ H returns true $\iff$ $D(\langle D \rangle)$ loops
$D(\langle D \rangle)$ loops $\iff$ H returns false $\iff$ $D(\langle D \rangle)$ halts.

A contradiction. No decider for H can exist and we see H is undecidable.