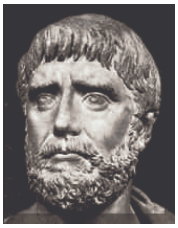
15-251

Some ~~Great~~ Theoretical Ideas ~~in~~ Computer Science for

Thales' and Gödel's Legacy: Proofs and Their Limitations

Lecture 26 (April 22, 2008)



Axioms

In traditional logic, an axiom or postulate is a proposition that is not proved or demonstrated but considered to be self-evident. Therefore, its truth is taken for granted, and serves as a starting point for deducing and inferring other truths.

Peano Arithmetic

The Peano axioms formally define the properties of the natural numbers

1. For every natural number n, n = n
2. For all natural numbers, if n = m, then m = n.
3. For all naturals if k = m and m = n then k = n.
4. If n is a natural number and n = m, then m is also a natural number.

5. 0 is a natural number.

6. For every natural number n, S(n) is a natural number.

7. For every natural number n, $S(n) \neq 0$.

8. For all natural numbers m and n, if S(m) = S(n), then m = n.

What is a proof?

Intuitively, a proof is a sequence of "statements", each of which follows "logically" from some of the previous steps.

What are "statements"? What does it mean for one to follow "logically" from another?

What are "statements"? What does it mean for one to follow "logically" from another?

Intuitively, statements must be stated in some language.

Formally, statements are strings of a decidable language S over Σ.

That is, S is a subset of Σ^* and there is a Java program $P_S(x)$ that outputs Yes if x is in S, and outputs No otherwise.

This decidable set S is the set of "syntactically valid" strings, or "statements" of a language.

Example:
Let S be the set of all syntactically well formed statements in propositional logic.

$X \vee \neg X$
$(X \wedge Y) \Rightarrow Y$
$\vee X \neg Y$ (not)

Typically, language syntax is defined inductively.

This makes it easy to write a recursive program to recognize the strings in the language.

Syntax for Statements in Propositional Logic

Variable $\rightarrow$ X, Y, X_1, X_2, X_3, …

Literal $\rightarrow$ Variable | $\neg$Variable

Statement $\rightarrow$
- Literal
- $\neg$(Statement)
- Statement $\wedge$ Statement
- Statement $\vee$ Statement

Recursive Program to decide S

ValidProp(S) {
 return True if any of the following:

 S has the form $\neg(S_1)$ and ValidProp(S_1)
 S has the form ($S_1 \wedge S_2$) and
  ValidProp(S_1) AND ValidProp(S_2)
 S has the form …..

}

We can now precisely define a syntactically valid set of "statements" in a language.

But what is "logic", and what is "meaning"?

For the time being, let us ignore the meaning of "meaning", and pin down our concepts in purely symbolic (syntactic) terms.

Define a function $Logic_S$

Given a decidable set of statements S, fix any single computable "logic function":
 $Logic_S$: (S $\cup$ Δ) × S $\rightarrow$ Yes/No

If Logic(x,y) = Yes, we say that the statement y is implied by statement x.

We also have a "start statement" Δ not in S, where
 $Logic_S(\Delta,x)$ = Yes will mean that our logic views the statement x as an axiom.

A valid proof in logic $Logic_S$

A sequence $s_1, s_2, \ldots, s_n$ of statements is a valid proof of statement Q in $Logic_S$ iff

- $Logic_S(\Delta, s_1)$ = True
  (i.e., s_1 is an axiom of our language)
- For all $1 \leq i \leq n-1$, $Logic_S(s_j, s_{j+1})$ = True
  (i.e., each statement implies the next one)
- And finally, s_n = Q
  (i.e., the final statement is indeed Q.)

Provable Statements (a.k.a. Theorems)

Let S be a set of statements.
Let L be a logic function.

Define $Provable_{S,L}$ =
All statements Q in S for which there is a valid proof of Q in logic L.

Example $SILLY_1$

S = All strings.
L = All pairs of the form: $<\Delta, s>$, $s \in S$

$Provable_{S,L}$ is the set of all strings.

Example: $SILLY_2$

S = All strings over {0,1}.
L = $<\Delta, 0>$, $<\Delta, 1>$, and
all pairs of the form: <s,s0> or <s, s1>

$Provable_{S,L}$ is the set of all strings.

Example: SILLY$_3$

S = All strings.

L = <Δ, 0> , <Δ, 11>, and
all pairs of the form: <s,s0> or <st, s1t1>

Provable$_{S,L}$ is the set of all strings with an even number of 1s

Example: Propositional Logic

S = All well-formed formulas in the notation of Propositional Logic.

L = Two formulas are one step apart if one can be made from the other from a finite list of forms. (see next page for a partial list.)

Modus ponens
$[(p \to q) \wedge p] \to [q]$

Modus tollens
$[(p \to q) \wedge \neg q] \to [\neg p]$

Conjunction introduction (or *Conjunction*)
$[(p) \wedge (q)] \to [p \wedge q]$

Disjunction introduction (or *Addition*)
$[p] \to [p \vee q]$

Simplification
$[p \wedge q] \to [p]$

Disjunctive syllogism
$[(p \vee q) \wedge \neg p] \to [q]$

Hypothetical syllogism
$[(p \to q) \wedge (q \to r)] \to [p \to r]$

Constructive dilemma
$[(p \to q) \wedge (r \to s) \wedge (p \vee r)] \to [q \vee s]$

Destructive dilemma
$[(p \to q) \wedge (r \to s) \wedge (\neg q \vee \neg s)] \to [\neg p \vee \neg r]$
(The same as 2 applications of transposition, then 1 application of constructive dilemma.)

Resolution
$[(p \vee q) \wedge (\neg p \vee r)] \to [(q \vee r)]$

Absorption

Example: Propositional Logic

S = All well-formed formulas in the notation of Propositional Logic.

L = Two formulas are one step apart if one can be made from the other from a finite list of forms. (see previous page for a partial list.)

(hopefully) Provable$_{S,L}$ is the set of all formulas that are tautologies in propositional logic.

Super Important Fact

Let S be any (decidable) set of statements.

Let L be any (computable) logic.

We can write a program to enumerate the provable theorems of L.

I.e., $Provable_{S,L}$ is enumerable.

Enumerating the Set $Provable_{S,L}$

```
for k = 0 to forever do
{
  let PROOF loop through all strings of length k
  {
     let STMT loop through all strings of length < k
     {
       if proofcheck_S,L(STMT, PROOF) = Valid
       {
          output STMT;                //this is a theorem
       }
     }
  }
}
```

Example: Euclid and ELEMENTS

We could write a program ELEMENTS to check (STATEMENT, PROOF) pairs to determine if PROOF is a sequence, where each step is either one logical inference, or one application of the axioms of Euclidian geometry.

$THEOREMS_{ELEMENTS}$ is the set of all statements provable from the axioms of Euclidean geometry.

Example: Peano and PA.

We could write a program PA to check (STATEMENT, PROOF) pairs to determine if PROOF is a sequence, where each step is either one logical inference, or one application of the axioms of Peano Arithmetic

$THEOREMS_{PA}$ is the set of all statements provable from the axioms of Peano Arithmetic

OK, so I see what valid syntax is, what logic is, what a proof and what theorems are…

But where does "truth" and "meaning" come in it?

Let S be any decidable language. Let Truth_S be any fixed function from S to True/False.

We say Truth_S is a "truth concept" associated with the strings in S.

Truths of Natural Arithmetic

Arithmetic_Truth =

All TRUE expressions of the language of arithmetic (logical symbols and quantification over Naturals).

Truths of Euclidean Geometry

Euclid_Truth =

All TRUE expressions of the language of Euclidean geometry.

Truths of JAVA Program Behavior

JAVA_Truth =

All TRUE expressions of the form program "P on input X will halt" or "not halt"

General Picture

A decidable set of statements S.

A computable logic L.

A (possibly uncomputable) truth concept
$Truth_S: S \rightarrow \{T, F\}$

We work in logics that we think are related to our truth concepts.

A logic L is "sound" for a truth concept $Truth_S$ if

x in $Provable_{S,L} \Rightarrow Truth_S(x) = T$

L is sound for $Truth_S$ if

- $L(\Delta, A) = true \Rightarrow Truth_S(A) = True$
- $L(B,C)=True$ and $Truth_S(B)=True \Rightarrow Truth_S(C)= True$

L is sound for $Truth_S$ means that L can't prove anything false for the truth concept $Truth_S$.

$Provable_{L,S} \Rightarrow Truth_S$

$SILLY_3$ is sound for the truth concept of an even number of ones.

Example $SILLY_3$

S = All strings.
L = <Δ, 0> , <Δ, 11>, and
all pairs of the form: <s,s0> or <st, s1t1>

$Provable_{S,L}$ is the set of all strings with zero parity.

Euclidean Geometry is sound for the truth concept of facts about points and lines in the Euclidean plane.

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

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

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

Soundness:
$Provable_{S,L} \Rightarrow Truth_S$

Completeness:
$Truth_S \Rightarrow Provable_{S,L}$

$SILLY_3$ is sound and complete for the truth concept of an even number of ones.

Example $SILLY_3$

S = All strings.
L = <Δ, 0> , <Δ, 11>, and
all pairs of the form: <s,s0> or <st, s1t1>

$Provable_{S,L}$ is the set of all strings with zero parity.

Truth versus Provability

Happy News:

$Provable_{Elements}$ = Euclid_Truth

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

Truth versus Provability

Sucky Fact:

$Provable_{PeanoArith}$ is a proper subset of Arithmetic_Truth

Peano Arithmetic is sound.
It is not complete.

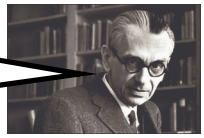
Truth versus Provability

Foundational Crisis:

It is impossible to have a proof system F such that

$Provable_{F,S}$ = Arithmetic_Truth

F is sound for arithmetic will imply F is not complete.



Here's what we have

A language S.

A truth concept $Truth_S$.

A logic L that is sound (maybe even complete) for the truth concept.

An enumerable list $Provable_{S,L}$ of provable statements (theorems) in the logic.

JAVA_Truth is Not Enumerable

Suppose JAVA_Truth is enumerable, and the program JAVA_LIST enumerates JAVA_Truth.

Can now make a program HALT(P):

Run JAVA_LIST until either of the two statements appears: "P(P) halts", or "P(P) does not halt".

Output the appropriate answer.

Contradiction of undecidability of K.

JAVA_Truth has No Proof System

There is no sound and complete proof system for JAVA_Truth.

Suppose there is. Then there must be a program to enumerate $Provable_{S,L}$.

$Provable_{S,L}$ is recursively enumerable.

JAVA_Truth is not recursively enumerable.

So $Provable_{S,L} \neq$ JAVA_Truth

The Halting problem is not decidable.

Hence, JAVA_Truth is not recursively enumerable.

Hence, JAVA_Truth has no sound and complete proof system.

Similarly, in the last lecture, we saw that the existence of integer roots for Diophantine equations was not decidable.

Hence, Arithmetic_Truth is not recursively enumerable.

Hence, Arithmetic_Truth has no sound and complete proof system!!!!

Hilbert's Second Question [1900]

Is there a foundation for mathematics that would, in principle, allow us to decide the truth of any mathematical proposition? Such a foundation would have to give us a clear procedure (algorithm) for making the decision.

Hilbert

Foundation F

Let F be any foundation for mathematics:

1. F is a proof system that only proves true things [Soundness]

2. The set of valid proofs is computable. [There is a program to check any candidate proof in this system]

(Think of F as (S,L) in the preceding discussion, with L being sound.)

Gödel's Incompleteness Theorem

In 1931, Kurt Gödel stunned the world by proving that for any consistent axioms F there is a true statement of first order number theory that is not provable or disprovable by F.

I.e., a true statement that can be made using 0, 1, plus, times, for every, there exists, AND, OR, NOT, parentheses, and variables that refer to natural numbers.

Incompleteness

Let us fix F to be any attempt to give a foundation for mathematics. We have already proved that it cannot be sound and complete. Furthermore…

We can even construct a statement that we will all believe to be true, but is not provable in F.

$CONFUSE_F(P)$

Loop though all sequences of sentences in S

If S is a valid F-proof of "P halts", then loop-forever

If S is a valid F-proof of "P never halts", then halt.

Program $CONFUSE_F(P)$

Loop though all sequences of sentences in S
If S is a valid F-proof of "P halts", then loop-forever
If S is a valid F-proof of "P never halts", then halt.

$GODEL_F$ = AUTO_CANNIBAL_MAKER($CONFUSE_F$)

Thus, when we run $GODEL_F$ it will do the same thing as:

$CONFUSE_F(GODEL_F)$

Program $CONFUSE_F(P)$ Loop though all sequences of sentences in S If S is a valid F-proof of "P halts", then loop-forever If S is a valid F-proof of "P never halts", then halt.	$GODEL_F$ = AUTO_CANNIBAL_MAKER($CONFUSE_F$) Thus, when we run $GODEL_F$ it will do the same thing as $CONFUSE_F(GODEL_F)$

Can F prove $GODEL_F$ halts?

If Yes, then $CONFUSE_F(GODEL_F)$ does not halt: Contradiction

Can F prove $GODEL_F$ does not halt?

If Yes , then $CONFUSE_F(GODEL_F)$ halts: Contradiction

$GODEL_F$

F can't prove or disprove that $GODEL_F$ halts.

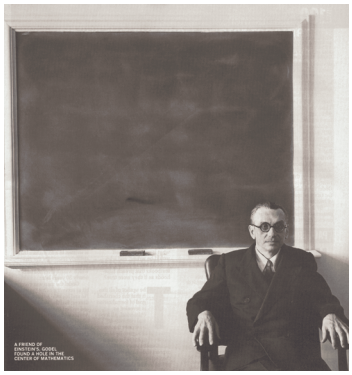
But $GODEL_F = CONFUSE_F(GODEL_F)$ is the program:

Loop though all sequences of sentences in S

If S is a valid F-proof of "$GODEL_F$ halts", then loop-forever

If S is a valid F-proof of "$GODEL_F$ never halts", then halt.

And this program does not halt!



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

In particular, it can't prove the true statement that $GODEL_F$ does not halt.

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!