MATH

Some AWESOME

~~Great Theoretical Ideas~~

~~Some Formal Logic~~

~~in Computer Science~~

(which is really Math, but has applications in Computer Science)

about ~~Generating Functions~~

~~Probability~~

~~Infinity~~

Computability

With Alan! (not Turing)

Formal Logic, Why Gödel was Awesome, And Some Harsh Truths

Lecture 25 (April 20, 2010)

Adam Blank

$$\text{Let L} = \{l | l \text{ is a 15-251 lecture}\}$$
$$\text{Let S} = \{s | s \text{ is a 15-251 student}\}$$
$$\text{Let } xIy \text{ stand for } x \text{ is interested by } y$$

$$\forall (l \in L) \exists (s \in S) \sim sIl$$

Announcements

You are now breathing manually MOAR.

Homework 9 is due THURSDAY.

Homework 10 will be out TONIGHT.

The last quiz is on Thursday!

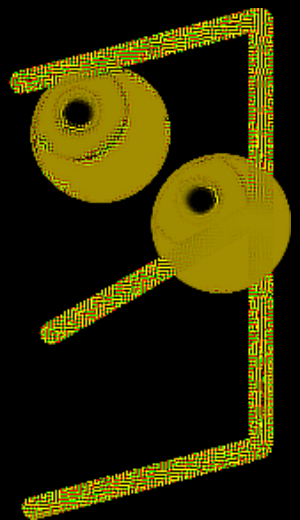
Let's go to
First-Order Logic Land

Four-Eyes AI

I've booked us a tour!

Ida Stencil

...But wait...
We need to go through
Propositional Calculus
Pathway



A Logistic System Named $\mathcal{P}$

A **proposition** is a statement that has a truth value.

Some examples:

"Adam is currently giving a 15-251 lecture."

"Danny is currently giving a 15-251 lecture."

Some non-examples:

"Apples taste good."

"Grapes make five."

A Logistic System Named $\mathcal{P}$

Propositional Variables represent propositions. We usually use letters like $\mathtt{p}$, $\mathtt{q}$, or $\mathtt{r}$ as propositional variables.

p = "Adam is currently giving a 15-251 lecture."

q = "Danny is currently giving a 15-251 lecture."

We let bolded (or underlined) letters represent arbitrary propositions.

p, **q**, **r**

A Logistic System Named $\mathcal{P}$

Intuitively, $\mathcal{P}$ lets us represent **relations** between propositions.

p = "Adam is currently giving a 15-251 lecture."

q = "Danny is currently giving a 15-251 lecture."

…A quick aside to some notation…

Some Important Notation: Logical Connectives

$\sim \mathrm{p}$	The negation of **p**
$\mathrm{p} \vee \mathrm{q}$	Either **p**, **q**, or both
$\mathrm{p} \wedge \mathrm{q}$	Both **p** and **q**
$\mathrm{p} \supset \mathrm{q}$	If **p**, then **q**
$\mathrm{p} \equiv \mathrm{q}$	**p** if and only if **q**

Some Important Notation: Abbreviations

We can define all boolean operations in terms of just negation and disjunction. So, $\{\sim, \vee\}$, is said to be a **complete** set of logical connectives.

$$[p \supset q] \leftrightarrow [\sim p \vee q]$$

$$[p \wedge q] \leftrightarrow \sim [\sim p \vee \sim q]$$

$$[p \equiv q] \leftrightarrow [[p \supset q] \wedge [q \supset p]]$$

A Logistic System Named $\mathcal{P}$

Intuitively, $\mathcal{P}$ lets us represent **relations** between propositions.

p ="Adam is currently giving a 15-251 lecture."

q ="Danny is currently giving a 15-251 lecture."

$p \supset\sim q$

$p \vee q$

p

$\sim q$

A Logistic System Named $\mathcal{P}$

Let's formally define $\mathcal{P}$.

$\mathcal{P}$ is a language. So, it has **syntax** and **semantics**. These are DISTINCT! First, we define the syntax.

Primitive Symbols of $\mathcal{P}$:

$$[\ ]\sim\vee$$

$$p, q, r, p_1, q_1, r_1, \ldots$$

A Logistic System Named $\mathcal{P}$

Primitive Symbols of $\mathcal{P}$:

$[\ ]\ \sim\ \vee$

$p, q, r, p_1, q_1, r_1, \ldots$

Syntax of $\mathcal{P}$.

A **formula** is a finite string of primitive symbols.

Some Examples:

$]\sim pq\sim \qquad [\vee] \qquad [p \vee q]$

A **well-formed formula** or **wff** is a formula that can be formed using the following three "formation rules":

(We let capital bold letters stand for arbitrary wffs.)

(1) A propositional variable **p** is a wff.

(2) If A is a wff, then $\sim \mathrm{A}$ is a wff.

(3) If A and B are wffs, then $[\mathrm{A} \vee \mathrm{B}]$ is a wff.

A Logistic System Named $\mathcal{P}$

Well-Formed Formulae of $\mathcal{P}$:

(1) A propositional variable **p** is a wff.

(2) If A is a wff, then $\sim \mathrm{A}$ is a wff.

(3) If A and B are wffs, then $[\mathrm{A} \vee \mathrm{B}]$ is a wff.

Let's again take a step back and talk more generally…

Axioms, Provability, and Theorems

Let's look at an arbitrary axiomatic system $\mathcal{S}$.

The system $\mathcal{S}$ is characterized completely by the set of **axioms** and the set of **inference rules** that we take.

An **axiom** is a wff that we take to be immediately provable in $\mathcal{S}$.

Axioms, Provability, and Theorems

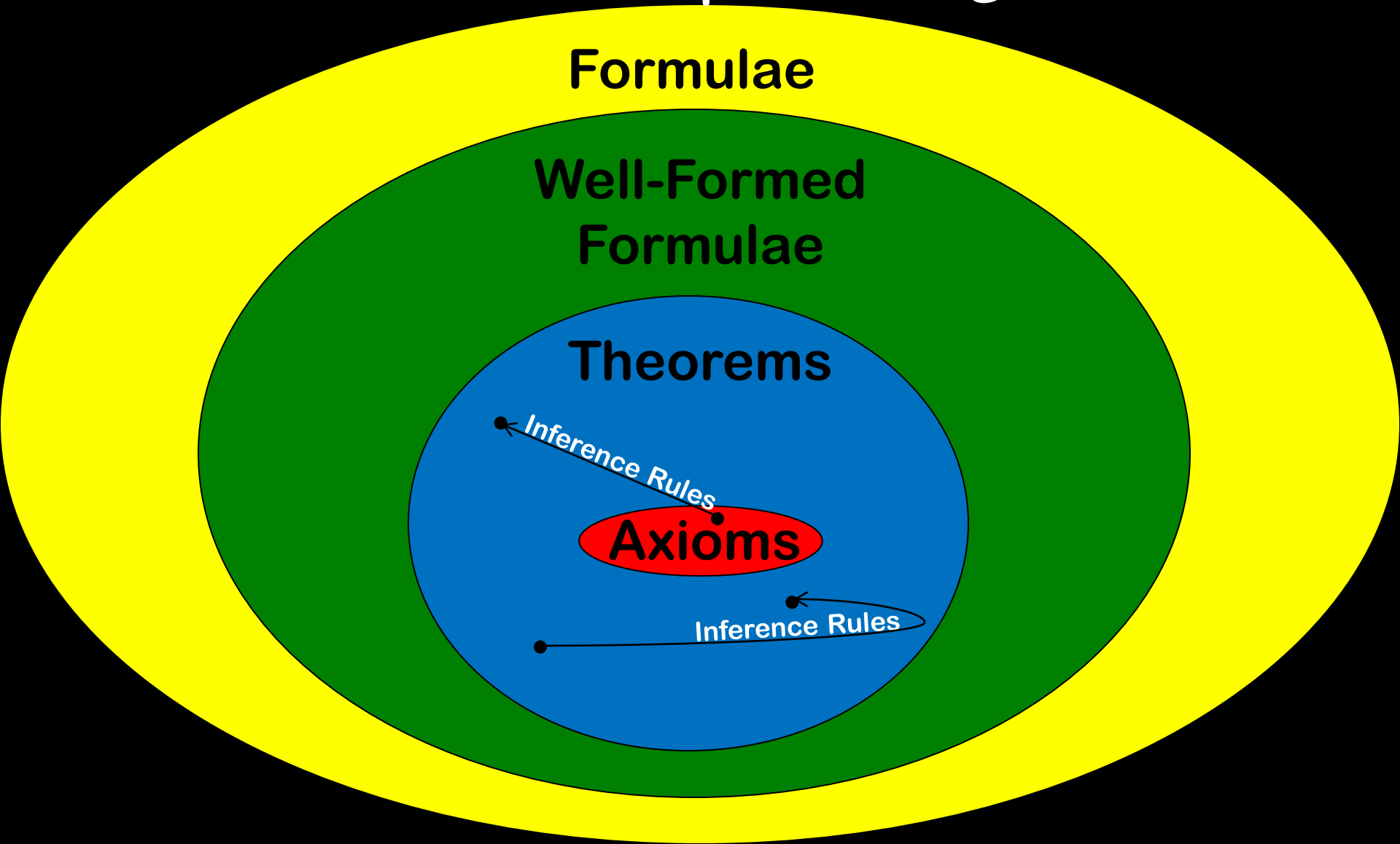
Let's look at an arbitrary axiomatic system $\mathcal{S}$.

The system $\mathcal{S}$ is characterized completely by the set of **axioms** and the set of **inference rules** that we take.

An **inference rule** is a way to prove new theorems using known theorems.

Axioms, Provability, and Theorems

How about a picture of $\mathcal{S}$?



A Logistic System Named $\mathcal{P}$

Well-Formed Formulae of $\mathcal{P}$:

(1) A propositional variable **p** is a wff.

(2) If A is a wff, then $\sim \mathrm{A}$ is a wff.

(3) If A and B are wffs, then $[\mathrm{A} \vee \mathrm{B}]$ is a wff.

Axiom Schemata of $\mathcal{P}$:

(Ax1) $[\mathrm{A} \vee \mathrm{A}] \supset \mathrm{A}$

(Ax2) $\mathrm{A} \supset [\mathrm{B} \vee \mathrm{A}]$

(Ax3) $[\mathrm{A} \supset \mathrm{B}] \supset [[\mathrm{C} \vee \mathrm{A}] \supset [\mathrm{B} \vee \mathrm{C}]]$

Inference Rules of $\mathcal{P}$:

(MP) From A and $\mathrm{A} \supset \mathrm{B}$, infer B.

A Logistic System Named $\mathcal{P}$

(Ax1) $[\mathbf{A} \vee \mathbf{A}] \supset \mathbf{A}$

(Ax2) $\mathbf{A} \supset [\mathbf{B} \vee \mathbf{A}]$

(Ax3) $[\mathbf{A} \supset \mathbf{B}] \supset [[\mathbf{C} \vee \mathbf{A}] \supset [\mathbf{B} \vee \mathbf{C}]]$

(MP) From $\mathbf{A}$ and $\mathbf{A} \supset \mathbf{B}$, infer $\mathbf{B}$.

Let's prove something in $\mathcal{P}$!

Theorem. $\vdash p \vee \sim p$

(1) $\vdash [\mathbf{A} \supset \mathbf{B}] \supset [[\mathbf{C} \vee \mathbf{A}] \supset [\mathbf{B} \vee \mathbf{C}]]$

(2) $\vdash [\mathbf{A} \supset \mathbf{B}] \supset [[\sim p \vee \mathbf{A}] \supset [\mathbf{B} \vee \sim p]]$

(3) $\vdash [\mathbf{A} \supset p] \supset [[\sim p \vee \mathbf{A}] \supset [p \vee \sim p]]$

(4) $\vdash [[p \vee p] \supset p] \supset [[\sim p \vee [p \vee p]] \supset [p \vee \sim p]]$ **Ax3**

(5) $\vdash [[p \vee p] \supset p$ **Ax1**

(6) $\vdash [\sim p \vee [p \vee p]] \supset [p \vee \sim p]$ **MP: 4,5**

(7) $\vdash \sim p \vee [p \vee p]$ **Ax2**

(8) $\vdash p \vee \sim p$ **MP: 6,7**

A Fundamental Theorem About Theorems

Principle of Induction on Proofs

Let $\mathcal{R}$ be a property.

If

1) $\mathcal{R}$ is true of all axioms of a system
2) $\mathcal{R}$ is "preserved" by all inference rules of the same system

Then

$\mathcal{R}$ is true of all theorems of that system

(The proof goes by strong induction on the proof of an arbitrary theorem in the logistic system, but is omitted for brevity.)

An Example of Induction on Proofs using $\mathcal{P}$

(Ax1) $[A \vee A] \supset A$

(Ax2) $A \supset [B \vee A]$

(Ax3) $[A \supset B] \supset [[C \vee A] \supset [B \vee C]]$

(MP) From A and $A \supset B$, infer B.

(Principle of Induction on Proofs)

Claim: All theorems have matched braces

Proof: By Induction on Proofs

Base Cases:

(Ax1) $[A \vee A] \supset A$

(Ax2) $A \supset [B \vee A]$

(Ax3) $[A \supset B] \supset [[C \vee A] \supset [B \vee C]]$

Induction Step:

(MP) $A \quad [\sim A \vee B] \longrightarrow B$

Semantics of Logistic Systems

Up until now, we've been building up the tools and resources necessary to describe the syntax of a logistic system…
But what about the semantics?

Consistency

Soundness

Completeness

Semantics of Logistic Systems

Consistency

Soundness

Completeness

There are many "types" of consistency.
These "types" of consistency are
properties that a logistic system can have.

Absolute Consistency means that not all wffs are provable in the logistic system.

Consistency with Respect to Negation means that it is not the case that any wff and its negation are both provable in the logistic system.

Semantics of Logistic Systems

Consistency Absolute Consistency means that not all wffs are provable in the logistic system.

Soundness

Completeness

A logistic system is **sound** if all provable wffs (that is, all theorems) are "true."

Semantics of Logistic Systems

Consistency Absolute Consistency means that not all wffs are provable in the logistic system.

Soundness A logistic system is sound if all provable wffs (that is, all theorems) are "true."

Completeness

A logistic system is **complete** if all "true" wffs are provable (that is, are theorems).

Notice that if a system is both sound and complete, then "truth" and "provability" are THE SAME THING!

Truth in $\mathcal{P}$

Well-Formed Formulae of $\mathcal{P}$:

(1) A propositional variable **p** is a wff.

(2) If A is a wff, then $\sim \mathrm{A}$ is a wff.

(3) If A and B are wffs, then $[\mathrm{A} \vee \mathrm{B}]$ is a wff.

We reason about the "truth" of wffs using the concept of assignments. An **assignment** gives a truth value to every propositional variable in the wff.

$\sim \mathrm{A}$ is true if and only if A is not true.

$[\mathrm{A} \vee \mathrm{B}]$ is true if and only if either A is true or B is true.

A wff is a **tautology** if and only if it is true regardless of the assignment given to its propositional variables.

Soundness of $\mathcal{P}$

(Ax1) $[A \vee A] \supset A$

(Ax2) $A \supset [B \vee A]$

(Ax3) $[A \supset B] \supset [[C \vee A] \supset [B \vee C]]$

(MP) From A and $A \supset B$, infer B.

(Principle of Induction on Proofs)

Claim: All theorems of $\mathcal{P}$ are tautologies

Proof: By Induction on Proofs

Base Cases:

(Ax1) $[A \vee A] \supset A$

(Ax2) $A \supset [B \vee A]$

(Ax3) $[A \supset B] \supset [[C \vee A] \supset [B \vee C]]$

Induction Step:

(MP) $A \quad [A \supset B] \longrightarrow B$

Consistency of $\mathcal{P}$

Theorem: All theorems of $\mathcal{P}$ are tautologies.

Claim: $\mathcal{P}$ is consistent with respect to negation.

Proof: Let A be an arbitrary theorem of $\mathcal{P}$. Then, by the soundness theorem, it is a tautology. Observe that $\sim \mathrm{A}$ is false, regardless of the assignment to propositional variables. Then, it is clearly not a tautology.

Claim: $\mathcal{P}$ is absolutely consistent .

Proof: This follows from the above.

Completeness of $\mathcal{P}$

Recall that completeness means that every "true" statement is provable.

For $\mathcal{P}$, that is the same as saying all tautologies are provable.

The proof of completeness is not much harder, but is left as an exercise to the audience.

Are we there yet?

$\mathcal{F}$irst order logic

A small extension to $\mathcal{P}$

What happened to us??

Well-Formed Formulae of $\mathcal{P}$:

(1) A propositional variable **p** is a wff.

(2) If A is a wff, then $\sim \mathrm{A}$ is a wff.

(3) If A and B are wffs, then $[\mathrm{A} \vee \mathrm{B}]$ is a wff.

Axiom Schemata of $\mathcal{P}$:

(Ax1) $[\mathrm{A} \vee \mathrm{A}] \supset \mathrm{A}$

(Ax2) $\mathrm{A} \supset [\mathrm{B} \vee \mathrm{A}]$

(Ax3) $[\mathrm{A} \supset \mathrm{B}] \supset [[\mathrm{C} \vee \mathrm{A}] \supset [\mathrm{B} \vee \mathrm{C}]]$

Axioms for quantifiers

Inference Rules of $\mathcal{P}$:

(MP) From A and $\mathrm{A} \supset \mathrm{B}$, infer B.

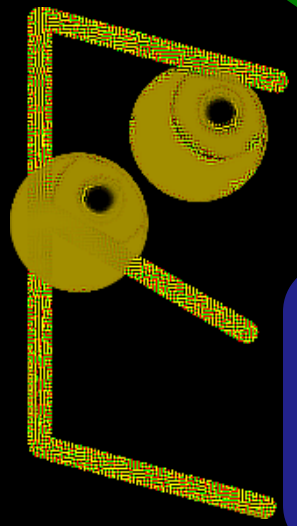
Inference Rule for Generalization with Quantifiers

Remember $\mathcal{P}$?

$\mathcal{F}$ is what results if we add **quantifiers** and **individuals**.

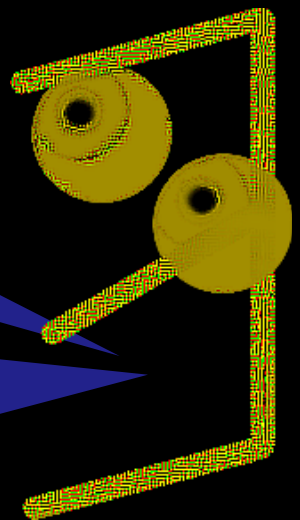
Yay! First-Order Logic!

Then we get ARITHMETIC!



OH NO!!! Not Arithmetic!!!
AHHHHHH!!!!!

What happens if we spec[illegible]
the individuals to be natural
numbers?!?!?!



Let's start $\mathcal{A}$/Over Again

Primitive Symbols of $\mathcal{A}$:

$$0\ `\ [\ ]\ f\ p\ v\ ,\ \#\ \forall$$

Abbreviations (and definitions):

$f,$	$+$
$f,,$	$*$
$f,,,$	$\hat{}$

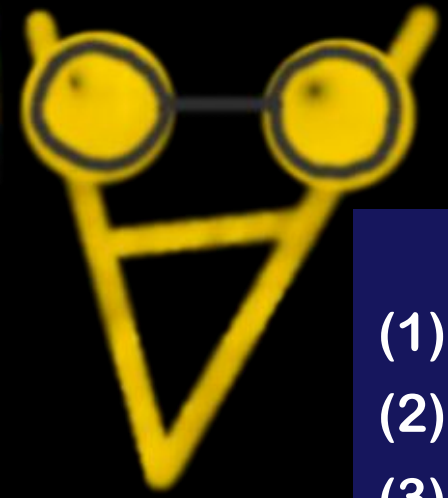
$p,$	$=$
$p,,$	$\sim$
$p,,,$	$\vee$

Primitive Functions in $\mathcal{A}$

Define S(n) to be the function that takes a natural and outputs its encoding in $\mathcal{A}$.

S(5) = 0’’’’’

We have to define the behavior of the primitive functions addition, multiplication, exponentiation. This is another inductive definition. It is omitted for brevity.



Formulae in $\mathcal{A}$

Terms of $\mathcal{A}$:

(1) Variables and Numerals are terms.

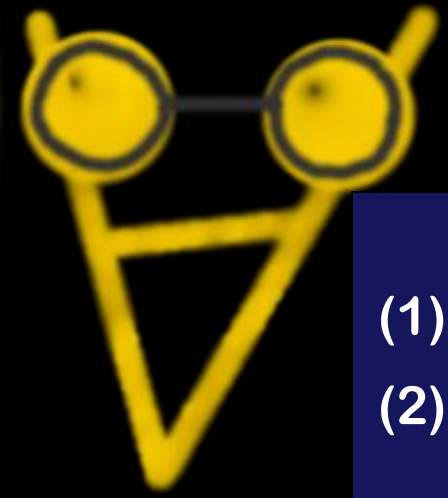
(2) If t_1 is a term, then t_1‘ is a term.

(3) If t_1 and t_2 are terms:
Then $[t_1 + t_2]$ is a term,
And $[t_1 * t_2]$ is a term,
And $[t_1 \hat{} t_2]$ is a term.

Well-Formed Formulae of $\mathcal{A}$:

(1) If t_1 and t_2 are terms, then $[t_1 = t_2]$ is a wff.

(2) If A and B are wffs:
Then $\sim \mathrm{A}$ is a wff,
And $[\mathrm{A} \vee \mathrm{B}]$ is a wff,
And for each variable v_i, $\forall v_i \mathrm{A}$ is a wff.



Truth in $\mathcal{A}$

Well-Formed Formulae of $\mathcal{A}$:

(1) If t_1 and t_2 are terms, then $[t_1 = t_2]$ is a wff.

(2) If A and B are wffs:
Then $\sim \mathrm{A}$ is a wff,
And $[\mathrm{A} \vee \mathrm{B}]$ is a wff,
And for each variable v_i, $\forall v_i \mathrm{A}$ is a wff.

$[c_1 = c_2]$ is true if and only if c_1 and c_2 refer to the same natural number.

$\sim \mathrm{A}$ is true if and only if A is not true.

$[\mathrm{A} \vee \mathrm{B}]$ is true if and only if either A is true or B is true.

$\forall v_i \mathrm{A}$ is true if and only if for every number n, replacing all occurrences of v_i "belonging" to the quantifier with n results in a true sentence.

Axioms of $\mathcal{A}$

Axiom Schemata of $\mathcal{P}$:

(Ax1) $[\mathbf{A} \vee \mathbf{A}] \supset \mathbf{A}$

(Ax2) $\mathbf{A} \supset [\mathbf{B} \vee \mathbf{A}]$

(Ax3) $[\mathbf{A} \supset \mathbf{B}] \supset [[\mathbf{C} \vee \mathbf{A}] \supset [\mathbf{B} \vee \mathbf{C}]]$

Axioms for quantifiers

Peano Axiomatization

Axioms for Equality

Axioms for Natural Numbers

1) 0 is a natural
2) n' is a natural
3) 0 is not the successor of any natural
4) ...

Axioms for Induction

Robinson Axiomatization

The First of Several Inconvenient Truths

Godel's First Incompleteness Theorem:

No recursively enumerable system capable of expressing arithmetic can be both consistent and complete.

We will prove the slightly weaker statement:
$\mathcal{A}$ with appropriate axiom schemata and inference rules cannot be consistent and complete.

The First of Several Inconvenient Truths

Godel's First Incompleteness Theorem:

No recursively enumerable system capable of expressing arithmetic can be both consistent and complete.

The Plan:

1) Express "provability" using arithmetic operations

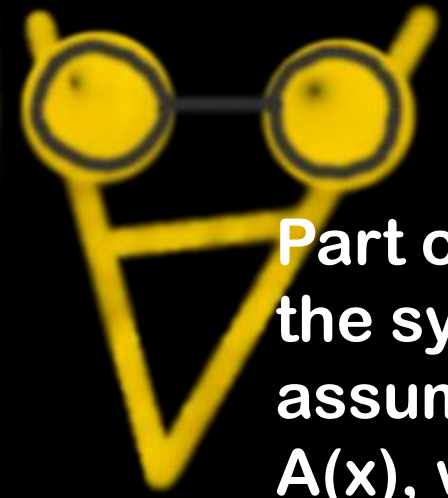
2) Create a "self-referential" sentence that describes its own non-provability

Gödel Numbering

F	0	$‘$	$[$	$]$	f	p	v	$,$	$\#$	$\forall$
	1	0	2	3	4	5	6	7	8	9

$$G(a_1 a_2 a_3 \ldots) = F(a_1)F(a_2)F(a_3)\ldots$$

The output of the function G is called a Gödel Numbering of the syntax of our system. Note that since we have 10 symbols, we can just concatenate the individual symbol numbers together to form the Gödel Number for a formula.



Arithmetization of Provability

Part of the concept of provability is the axioms of the system. Rather than explicitly choose axioms, we assume that they have been arithmetized into a wff A(x), where A(x) is true iff x is the Gödel Number of an axiom.

Ultimately, we want a wff: $P(g)$ is $\exists y[\mathrm{Pf}(y) \wedge g \in y]$
To get there, we formally define tuples using the # character. Given that we have tuples (and wffs to check if a tuple contains something), we can define Gödel Numbers of proofs!

To give an idea of what it is like, here is the arithmetization of a really primitive idea, "a string y ends in x": $xEy \leftrightarrow [x = y] \vee \exists z F(z) F(x) = y$

Diagonal Lemma

Let X(a) be a wff with exactly one variable not bound by a quantifier.

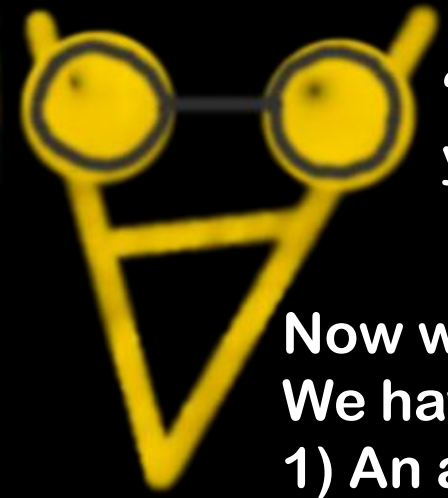
Claim: There exists a sentence Q, such that $Q \equiv X(G(Q))$ is provable.

Let $T(x) = \forall y[y = S(G(xG(x))) \supset X(y)]$

$Q = T(S(G(T)))$

$Q \equiv \forall y[y = S(G(TG(T))) \supset X(y)]$

Go by cases.
Case 1: Assume Q; substitute G(TS(G(T))) for y.
Case 2: Assume T(S(G(T)))

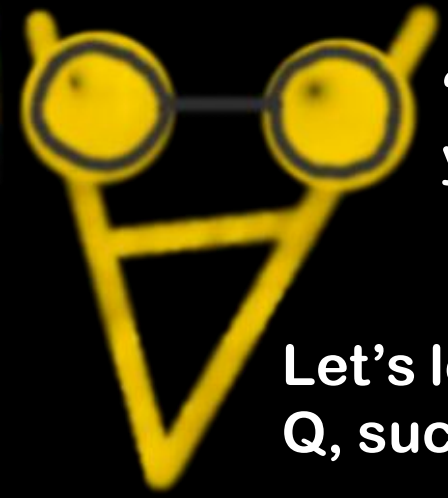


"yields falsehood when appended to its own quotation"
yields falsehood when appended to its own quotation

Now we're ready to prove the first incompleteness theorem!
We have:
1) An arithmetization of the concept of provability in the form of a wff P(g)
2) We know that there exists a sentence Q such that $Q \equiv X(G(Q))$ is provable.

Let's let X be $\sim P$. Now we know that there is a sentence Q, such that $Q \equiv \sim P(G(Q))$ is provable.

That is…there is a sentence that is true if and only if its Gödel Number is not provable…



"yields falsehood when appended to its own quotation" yields falsehood when appended to its own quotation

Let's let X be $\sim P$. Now we know that there is a sentence Q, such that $Q \equiv \sim P(G(Q))$ is provable.

This is going to be a contradiction proof. Assume for the sake of contradiction that $\mathcal{A}$ is both consistent and complete.

Suppose Q were provable. Then, P(G(Q)) would be provable, because a proof definitely exists. But Q is true iff G(Q) is not provable. This is a contradiction.

Now suppose Q were not provable. Then, P(G(Q)) would not be provable, because a proof definitely doesn't exist. But Q is false iff G(Q) is provable. This is a contradiction.

But wait! If Q isn't provable (which we just showed), then it's true!

MORE Inconvenient Truths

Godel's FIRST Incompleteness Theorem:

No recursively enumerable system capable of expressing arithmetic can be both consistent and complete.

Godel's SECOND Incompleteness Theorem:

No recursively enumerable system capable of expressing arithmetic can prove its own consistency…and remain consistent.

MORE Inconvenient Truths

Graph Minor Theorem

Continuum Hypothesis

Another Type of Logic

Intuitionistic Logic (also called **Constructive Logic**) is another type of logic that focuses on inference rules and does not take any axioms.

In Classical Logic, which is what we've been discussing, the goal is to formalize theories.

In Intuitionistic Logic, theorems are viewed as programs. They give explicit evidence that a claim is true.

Another Type of Logic

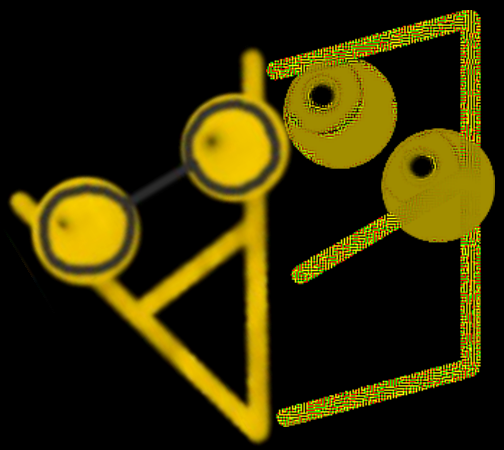
Intuitionistic Logic (also called **Constructive Logic**) is another type of logic that focuses on inference rules and does not take any axioms.

This means that there is no concept of "Proof by Contradiction."

Remember the theorem we proved in $\mathcal{P}$? $p \vee \sim p$

This is explicitly NOT a theorem in intuitionistic logics. Other than this theorem (and logically equivalent theorems, the two types of logics are identical.

Formal Logic / Gödel's Theorems



Here's What You Need to Know…

- Basic Propositional Calculus
- What consistency means
- What soundness means
- What completeness means
- Gödel's Incompleteness Theorems