8/22/2025
Proof and Problem Solving
Class Notes

INTRODUCTION TO SET THEORY AND LOGIC

Some background on logic and sets

- Set theory and logic together were used to provide a rigorous foundation for math
- Logicians also were able to find the limitations of logic and mathematical structures
- Removing parallel lines axiom from geometry and replacing it with a suitable axiom results in non-Euclidean geometry. Shows that a mathematical system depends on its axioms.
- Godel's incompleteness theorem showed further limitations (but not same as dependence of system on axiom)
- But once you know the limitations, you have a very good foundation

Background (contd)

- With such a firm foundation, mathematics can be made almost mechanical
- In future (actually now!) computers could verify theorems and even come up with new ones
- Computers are a natural next step in this evolution of math. They are basically machines that can do math, and they also depend on math to do everything.

Socrates' Paradox

I know one thing …
that I know nothing

Sad reality:

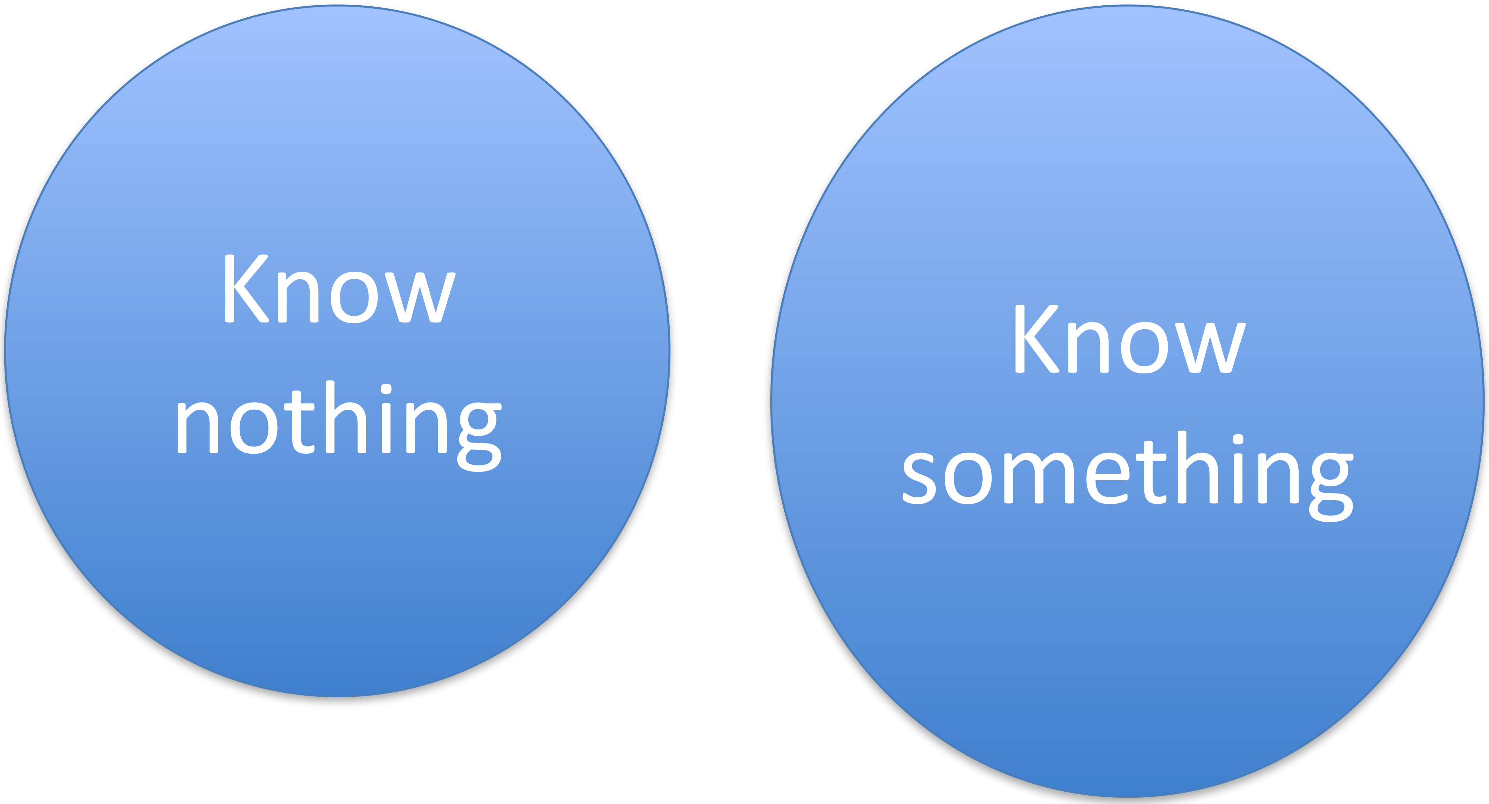
"The whole problem with the world is that fools and fanatics are always so certain of themselves, and wiser people so full of doubts." — Bertrand Russell

Different kinds of people

- A = Those who know that they know
- B = Those who know that they don’t know
- C = Those who don’t know that they know
- D = Those who don’t know that they don’t know

Socrates' Paradox in Set notation

- These sets have no intersection



Russell's paradox

- A barber is someone who shaves those and *only those* who do not shave themselves

- The set of all sets that are not members of themselves

- Such sets and statements are called "self-referential." The Zermelo-Frankel theory and the axiom of choice helped avoid this difficulty and created a proper foundation for logic. (Axiom is something assumed to be true)

Logical statements and proofs

- Al Gore “said” he invented the internet
- But he really didn’t
- He said that the climate is changing
- Therefore the climate is not changing

What is wrong with this “Proof” ?

LOGICAL CONNECTIVES AND QUANTIFIERS

$\neg \quad \vee \quad \wedge \quad \forall \quad \cup \quad \cap \quad \exists \quad \nexists \quad \rightarrow \quad \leftrightarrow$

$\neg$ is used in book for NOT

$\vee$ is used for OR

$\wedge$ is used for AND

$\forall$ means "For all"

$\rightarrow$ *or* $\Longrightarrow$ means "implies"

$\leftrightarrow$ *or* $\Longleftrightarrow$ means "if and only if"

Logical statements (propositions)

Write one of the logical statements above symbolically using NOT, AND, and OR operators and vice versa.

For example: If T means “Tax cuts” and E means “Economy Grows” then

$T \implies E$ means Tax cuts grow economy.

Negative of a statement

Negative of a statement: Opposite.

If one of them is true the opposite is false.

Example: Which of the following are opposite of "All men are created equal" ?

a. All women are created equal.
b. All men are not created equal.
c. Some men are better than others.
d. Not every man can run like Usain Bolt.

Negative - example

1. Example: Which of the following are opposite of "All men are created equal" ?
   a. All women are created equal.
   b. All men are not created equal.
   c. Some men are better than others.
   d. Not every man can run like Usain Bolt.

   Answer: only (b) is negative. (c) would be a negative if it said it said "Some men are created better than others."

   In symbols, negative of A -> B is A -> "NOT B"

DeMorgan's rule for logic

- "The sun is shining (S) and it is bright (B) can be written as $S \wedge B$
- What is its negative or opposite?
- Similarly, what is the negative of $S \vee B$?

De Morgan’s laws for logic

NOT(p OR q) ≡ (NOT p) AND (NOT q)

Where ≡ means “is equivalent to”

Using Truth Table

p	q	NOT(p or q)	(Not p) AND (Not q)
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

CONDITIONAL STATEMENTS
Converse of a statement

Example: If there is fire there will be smoke.

Converse: If there is smoke, there must be a fire.

Converse may not always be true.

In symbols, converse of A -> B is B -> A.

What is the opposite of this statement?

Equivalents of A -> B and B -> A

Verify the following using truth tables or other wise:

A implies B is equivalent to Not(B) implies Not (A)

(The second statement is the contrapositive)

Not (A implies B) is equivalent to “A and Not(B)”

So “A implies B” is equivalent to “Not(A) OR B”

Example of converse and contrapositive

We know, for functions,

differentiable -> continuous.

Converse: continuous -> differentiable (not always true).

Contrapositive: not continuous -> not differentiable (always true. In fact, contrapositives are always true).

Another way of stating it, using "A implies B" is equivalent to "Not(A) OR B" :

A function is either not differentiable or it is continuous.

Conditional statement EXAMPLE FERMAT’S THEOREM

- Let m,n,p,a,b all be natural numbers.
- Let P be the statement

  “n is a prime number”
- Let Q be the statement

  “$n = a^2+b^2$ for some a and b”
- Let R be the statement

  “ n is of the form 4m+1”

FERMAT’S THEOREM (page 2)

Fermat’s Theorem on sums of two squares

A prime number is a sum of two squares

if and only if

that prime number is of the form 4m+1

FERMAT'S THEOREM (page 3)

Fermat's Theorem in Symbols

$$(P \wedge Q) \leftrightarrow (P \wedge R)$$

FERMAT’S THEOREM (page 4)

Based on Fermat’s theorem, which of the following are true?

A. Every natural number that is a sum of two squares is a prime number
B. Every natural number of the form 4m+3 is not a sum of two squares
C. Every prime number of the form 4m+3 is not a sum of two squares
D. Every natural number of form 4m+1 is a sum of two squares.

Answers to questions from previous page

C is true and it is the contrapositive of the statement "P AND Q -> P AND R." More on that in an ensuing slide. A, B and D cannot be answered based only on Fermat's theorem's statement. The reason I put them there was twofold:

1. To show the scope of the statement and to show how to understand the scope of a statement.
2. To show some interesting facts from theory of numbers

So are A, B and D true or not?
(Just to pique your curiosity)

- Here is what is true (remember, this is outside the scope of the statement of Fermat's theorem, which is concerned with prime numbers):
- $25 = 4^2+5^2$, so that is a counter-example for A.
- 9 is not the sum of two squares, so that gives a counterexample for D. (0 is not a natural number).
- It is true that if n is of form 4m+3 then it is not the sum of two squares. Proof is elementary. Try!

p = sum of squares means p = 1 mod 4

Proof by contrapositive: Let p be odd, so p > 2.

Assume p is not = 1 mod 4. So p = 3 mod 4. Why?

Then we will show that p is not a sum of 2 squares.

If it were a sum of two squares, it has to be either 0 or 1 or 2 mod 4 because the square of any natural number is either 0 mod 4 if it is even

or 1 mod 4 if it is odd.

[Proof of previous statement: If m = 2k, then square is 4 times square of k. If m = 2k+1, then square is 1 + (4 times k times k+1)].

CONTRAPOSITIVE

CONTRAPOSITIVE

OF A

CONDITIONAL STATEMENT

IF P IMPLIES Q, THEN NOT Q IMPLIES NOT P

Example of contrapositives

Statement:

If sun I shining then it will be bright outside.

Contrapositive:

If it is not bright outside then sun is not shining.

Examples of converse and contrapositive

Write the converse and contrapositive for each:

1. If all roses are red, then all violets are blue.
2. $\forall x \in \mathbb{R}, x^2 > 4 \implies x > 2$

For 2, prove that it is false using a counterexample.

Difference between ≡ and ↔

p ≡ q means p and q are logically equivalent.

The statements always have the same logical value (T or F) regardless of the values of their components.

p↔ q (p iff q) is only concerned with the relationship – whether one implies the other.

Example in next page.

Difference between ≡ and $\leftrightarrow$: Example

- The statements “A implies B” and the statement “not B implies not A” are logically equivalent, regardless of what A and B are or whether A and B are true.
- But it would be silly to say “A implies B” iff “not B implies not A” even if that is true, because they are really two ways of saying same thing. (continued next page…

Difference between ≡ and ↔ : Example (cont.d from previous page)

On the other hand the two statements “P : The sun is shining” and “Q: It is daytime” are related by iff.

P↔Q because if sun is shining it is daytime and if it is daytime the sun must be shining. But we cannot say P ≡ Q. The two are not logically equivalent.

Being daytime is related to the sun shining but it is not just another way to say that the sun is shining.