Lecture 2

9/16

We will discuss the use of well-chosen words and symbols to express mathematical ideas precisely

Quantifiers and logical Statements

Def We use variables p, q, r to denote mathematical statements.
The truth or falsity of a statement is its truth value
Negating a statement reverses its truth value ($\neg p$ means "not p")

Def The universal quantifier for the variable x (written $\forall x \in S$ or "for all x in the set S) expresses that a predicate $P(x)$ can be satisfied by every member of the domain set S.

$$(\forall x \in S) P(x)$$

The existential quantifier for the variable x (written $\exists x \in S$ or "there exists an element x in the set S) expresses that a predicate $P(x)$ can be satisfied by at least one member of the domain set S.

$$(\exists x \in S) P(x)$$

English Words can Express Quantification

Universal ($\forall$)	(helpers)	Existential ($\exists$)	(helpers)
for all, for every	then	for some	such that
if		there exists	for which
whenever, for, given	satisfies	at least one	satisfies
every, any	must, is	some	such that
a, arbitrary	be	has a	
let			

Ex "The square of a real number is nonnegative"

$$\forall x \in \mathbb{R},\ x^2 \geq 0$$

Remark (Order of Quantifiers)

Consider the statement "If n is even, then n is the sum of two odd numbers".

Letting E and O be sets of even and odd integers, and letting $P(n,x,y)$ be $n=x+y$, the sentence becomes

$$(\forall n \in E)(\exists x,y \in O)\ P(n,x,y)$$

In this format the value chosen for a quantified variable remains unchanged for later expressions but can be chosen in terms of variables quantified earlier.

→ when we reach $(\exists x,y \in O)\ P(n,x,y)$ we treat "n" as a constant already chosen.

→ Same as in English, quantifiers appear in order at beginning of sentence so that the value of each variable is chosen independently of subsequently quantified variables.

Ex Compare the two statements

(i) $(\forall x \in A)(\exists y \in B)\ P(x,y)$ (ii) $(\exists y \in B)(\forall x \in A)\ P(x,y)$

Let $P(x,y)$ be "y is the parent of x". The first statement is true, but the second statement is too strong and is not true.

(i) For all x, there is a y such that y is the parent of x. (ii) There is a parent for all x such that y is the parent.

Remark (Negation of quantified statements)

$\neg((\forall x)\, P(x))$ has the same meaning as $(\exists x)(\neg P(x))$

$\neg((\exists x)\, P(x))$ has the same meaning as $(\forall x)(\neg P(x))$

When negating quantified statements with specified universes, one must not change the universe of potential values.

Ex (Negation involving universes)

The negation of "Every Good Boy Does Fine" is "some good boy does not do fine". It says nothing about bad boys.

The negation of "every chair in this room is broken" is "Some chair in this room is not broken". It says nothing about chairs outside this room.

Ex Negation of statement $(\forall n \in \mathbb{N})(\exists x \in A)(nx < 1)$ is $(\exists n \in \mathbb{N})(\forall x \in A)(nx \geq 1)$

The negated sentence means set A has a lower bound that is the reciprocal of an integer.

Ex Lets negate "every chair in this room is broken". Let R denote the set of classrooms. Given a room r, let $C(r)$ denote the set of chairs in r. For a chair c, let $B(c)$ be the statement that c is broken.

Then $\neg\{(\forall r \in R)(\exists c \in C(r))(\neg B(c))\} \Rightarrow (\exists r \in R)(\neg((\exists c \in C(r))(\neg B(c))$

Ex Lets negate the statement to write
"it is false that every classroom has a chair that is not broken."

Let: R denote the set of all classrooms

Given a room r, let $C(r)$ denote the set of chairs in r.

For a chair c, let $B(c)$ be the statement that c is broken.

The successive statements (all having the same meaning) become:

$$\neg \left[(\forall r \in R)\left((\exists c \in C(r)) (\neg B(c)) \right) \right]$$

$$(\exists r \in R) \left(\neg \left[(\exists c \in C(r)) (\neg B(c)) \right] \right)$$

$$(\exists r \in R) (\forall c \in C(r)) \, B(c)$$

Def (Logical Connectives)

Name	Symbol	Meaning	Condition for Truth
Negation	$\neg P$	not P	P false
Conjunction	$P \wedge Q$	P and Q	both true
Disjunction	$P \vee Q$	P or Q	at least one true
Biconditional	$P \Leftrightarrow Q$	P if and only if Q	same truth value
Conditional	$P \to Q$	P implies Q	Q true whenever P true

$P \Rightarrow Q$ P is called hypothesis, Q the Conclusion.

$Q \to P$ is <u>converse</u> of $P \to Q$

Ex (Truth Table)

P	Q	$P \to Q$	$\neg P$	$(\neg P) \vee Q$	R
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Suppose we want to check if the expression R given by $(P \to Q) \Leftrightarrow ((\neg P) \vee Q)$ is always true no matter what P and Q represent. This is called a tautology.

Construct the truth table and consider all cases.

Remark Elementary Logical Equivalency

a) $\neg(P \wedge Q)$ $\quad (\neg P) \vee (\neg Q)$

b) $\neg(P \vee Q)$ $\quad (\neg P) \wedge (\neg Q)$

c) $\neg(P \to Q)$ $\quad P \wedge (\neg Q)$

d) $P \Leftrightarrow Q$ $\quad (P \to Q) \wedge (Q \to P)$

e) $P \vee Q$ $\quad \neg P \to Q$

f) $P \Rightarrow Q$ $\quad \neg Q \to \neg P$

We also discussed the contrapositive $P \to Q$ is equivalent to $(\neg Q \to \neg P)$

Lets look at another example of <u>proof by contradiction</u>

<u>Thm</u> (Euclid) There are an infinite number of primes.

<u>Proof</u>

We will use two ideas

- The <u>Fundamental Theorem of Arithmetic</u> which states every integer greater than 1 can be expressed uniquely as a product of primes
- <u>Def</u> We say that $a|b$ or ("a divides b") if there exists some integer c such that $ac=b$. This means that an integer a divides a second integer b without producing a remainder.

We assume there is a finite number of primes.

Thus, we can enumerate the primes $p_1, p_2, \cdots, p_k$ with p_k representing the largest prime number

Define $N = p_1 \times p_2 \times p_3 \times \cdots \times p_k + 1$

By definition, N is an integer greater than 1 so it can be expressed uniquely as a product of primes.

Therefore, some prime number (p_1 through p_k) must divide N, or else N is a prime by definition itself.

However, when we check whether $p_1 | N$

$$\frac{N}{p_1} = \frac{p_1 \times p_2 \times p_3 \times \cdots \times p_K + 1}{p_1} = \frac{p_1 \times p_2 \times \cdots \times p_K}{p_1} + \frac{1}{p_1}$$

$$= p_2 \times p_3 \times \cdots \times p_K + \frac{1}{p_1}$$

We find that $p_1 \nmid N$ (p_1 does not divide N).

The same argument works for any p_i where $i = 1, \ldots, K$.

No prime number divides N, however this presents a contradiction.

By the Fundamental Theorem of Arithmetic, a prime number $p_1, \ldots, p_K$ must divide N or N is prime itself.

However, N is by definition bigger than p_K, so this is a contradiction. □

Lets look at an example.

Suppose $K = 5$ and there are only 5 primes

$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$

Then $N = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2{,}311$

$\frac{2{,}311}{2} = 1155.5$; ... $\frac{2311}{11} = 210.0909$

Since $\frac{N}{p_i}$ is never an integer (has a remainder), none of the primes divides N

Here N is a bigger prime (2311 is the 344th prime).

If we took $K = 6$, then $N = 30031$ which is composite. However, none of 2, 3, 5, 7, 11, 13 divide 30031. $59 | 30031$, and 59 is a larger prime, so again a contradiction.