Lecture - 14
Rule of Inference, Proofs

Translating Mathematical sentences into statements involving nested quantifiers: This will be illustrated by examples.

(1) Translate "The sum of two positive number is always positive."

Let us rewrite the above as follows; "For every two integers, if these integers are both positive, then the sum of these integers is positive."This can be expressed as

$$\forall x \forall y((x > 0) \wedge (y > 0) \to (x + y > 0)),$$

where the domain of discourse for both the variables is $\mathbb{Z}$.

(2) Express the definition of limit using quantifiers.
Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be a function. We say that f tends to a limit l as x tends to a, if for every real number $\epsilon > 0$ there exists a real number $\delta > 0$ such that $|f(x) - l| < \epsilon$ whenever $0 < |x - a| < \delta$. The above definition of limit can be expressed using quantifiers

$$\forall \epsilon \exists \delta \forall x(0 < |x - a| < \delta \to |f(x) - l| < \epsilon).$$

(3) Express the definition of convergence of a sequence using quantifiers.

Negating nested quantifiers: Recall the negation involving a single quantifier

Negation	Equivalent	When is Negation True?	When False?
$\neg \exists x P(x)$	$\forall x \neg P(x)$	For every $x, P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg \forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

To negate the statements involving nested quantifiers one has to successively apply the rules for negating statements involving a single quantifier.

(1) Negate the statement $\forall x \exists y(xy = 1)$ such that no negation precedes a quantifier.

We shall apply De Morgan's law successively for quantifiers so that we can move the negation $\neg \forall \exists (xy = 1)$ inside all the quantifiers.
$\neg \forall x \exists y(xy = 1)$ is equivalent to $\exists x \neg \exists y(xy = 1)$, which is equivalent to $\exists x \forall y \neg (xy = 1)$.
Now, $\neg(xy = 1)$ can be expressed as $xy \neq 1$. Therefore, we conclude that the negation of the given statement is $\exists x \forall y(xy \neq 1)$.

(2) Use quantifiers and predicates to express the fact that $\lim_{x \to a} f(x)$ does not exists.

This means that for all real numbers l, $\lim_{x\to a} f(x) \neq l$. Which can be expressed by the negation

$$\neg\forall\epsilon > 0\exists\delta > 0\forall x(0 < |x-a| < \delta \to |f(x)-l| < \epsilon).$$

$$\begin{aligned}
\neg\epsilon &> 0 \quad \exists\delta > 0\forall x(0 < |x-a| < \delta \to |f(x)-l| < \epsilon)\\
&\equiv \quad \exists\epsilon > 0\neg\exists\delta > 0\forall x(0 < |x-a| < \delta \to |f(x)-l| < \epsilon)\\
&\equiv \quad \exists\epsilon > 0\forall\delta > 0\neg\forall x(0 < |x-a| < \delta \to |f(x)-l| < \epsilon)\\
&\equiv \quad \exists\epsilon > 0\forall\delta > 0\exists\neg x(0 < |x-a| < \delta \to |f(x)-l| < \epsilon)\\
&\equiv \quad \exists\epsilon > 0\forall\delta > 0\exists x((0 < |x-a| < \delta) \land (|f(x)-l| \geq \epsilon))
\end{aligned}$$

Now, the statement "$\lim_{x\to a} f(x)$ does not exists" means that for all real numbers l, $\lim_{x\to a} f(x) \neq l$, and it can be expressed as

$$\forall l\exists\epsilon > 0\forall\delta > 0\exists x((0 < |x-a| < \delta) \land (|f(x)-l| \geq \epsilon)).$$

The above statement means that "for every real number l there is a real number $\epsilon > 0$ such that for every real number $\delta > 0$, there exists a real number x such that $0 < |x-a| < \delta$ and $|f(x)-l| \leq \epsilon$."

(3) Express "the sequence $\{x_n\}_{n\in\mathbb{N}}$ is not convergent" using quantifiers.

Rule of inference for quantified statements:

Rule of Inference	Name
$\dfrac{\forall x P(x)}{P(c)}$	Universal Instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\forall x P(x)}$	Universal generalization
$\dfrac{\exists x P(x)}{P(c) \text{ for some element } c}$	Existential Instantiation
$\dfrac{P(c) \text{ for some element } c}{\exists x P(x)}$	Existential generalization

Example: Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."

Let $C(x)$ be "x is in this class," $B(x)$ be "x has read the book," and $P(x)$ be "x passed the first exam."

Then the premises are $\exists x(C(x) \land \neg B(x))$ and $\forall x(C(x) \to P(x))$.

The conclusion is $\exists x(P(x) \land \neg B(x))$.

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential Instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal Instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	Existential generalization from (8)

Introduction to Proofs: We now discuss the notion of a proof and method of constructing proofs. A proof is a valid argument that establishes the truth of a mathematical statement. It uses the hypotheses of the theorem, if any, axioms assumed to be true, and previously known theorems.

The proof which we have seen earlier is called formal proof, where we used all the hypotheses and rules were acknowledged. Formal proofs can be very long and hard to follow. Therefore, we move from formal proofs towards informal proofs. In informal proofs more tahn one rule of of inference can be used in each step, and also the well understood steps may be skipped.

- **Theorem:** A theorem is a statement that can be shown true.
- **Proposition, Lemma:** A less important theorem.
- **Proof:** A proof is a valid argument that establishes the truth of a theorem.
- **Corollary:** A theorem that can be established directly from an already proved theorem.
- **Conjecture:** A statement that is being proposed to be true on the basis of some practical evidences.

Methods of proving Theorems: To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, we need to show that $P(a) \rightarrow Q(a)$, for an arbitrary element a in the domain, and then apply universal generalization.

Direct Proofs: A direct proof of a conditional statement $P \rightarrow Q$ involves the following; the first step is the assumption that p is true and then use the rule of inference and previously proven theorem to conclude that Q is also true in the final step.

"If n is an odd integer then so is the integer n^2."

Proof by Contraposition: This method use the fact that $P \rightarrow Q$ is equivalent to $\neg Q \rightarrow \neg P$. Thus, the conditional $P \rightarrow Q$ can be proved by showing that its contrapositive $\neg Q \rightarrow \neg P$ is true. To prove $\neg Q \rightarrow \neg P$ we use the method of direct proof.

Example: Let a, b, and n be positive integers. If $n = ab$, then $a \leq \sqrt{n}, b \leq \sqrt{n}$.

We prove by contraposition. Assume that $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$ is false. Which means that $a > \sqrt{n}, b > \sqrt{n}$ and this implies that $ab > n$. Thus we have shown that contrapositive is true hence the statement is also true.

Vacuous or trivial proofs: A proof of $P \to Q$ is true based on the fact that P is false.

Proof by contradiction: Suppose we want to prove that P is true. If we can find a contradiction Q such that $\neg P \to Q$ is true.Since Q is already known to be false, but $\neg P \to Q$. Therefore, we conclude that $\neg P$ is false and hence P is true.

Example: $\sqrt{2}$ is irrational.

Proof of equivalence: To prove a biconditional $P \leftrightarrow Q$, we show that $P \to Q$ and $Q \to P$ are both true, because

$$P \leftrightarrow Q \iff (P \to Q) \wedge (Q \to P).$$

Sometimes a theorem states that several statements are equivalent. viz. the following statements are equivalent $P_1, P_2, \cdots, P_n$. This can be written as $P_1 \leftrightarrow P_2 \cdots \leftrightarrow P_n$.
This means that all these statements ahave same truth value or equivalently, $P_i \leftrightarrow P_j$ for $1 \leq i, j \leq n$.
We shall use the following to prove such theorems;

$$P_1 \leftrightarrow P_2 \cdots \leftrightarrow P_n \iff ((P_1 \leftrightarrow P_2) \wedge (P_2 \leftrightarrow P_3) \wedge \cdots \wedge (P_n \leftrightarrow P_1)).$$

This means that if we show that $P_1 \leftrightarrow P_2, P_2 \leftrightarrow P_3, \cdots P_n \leftrightarrow P_1$ are all true then $P_1, P_2, \cdots P_n$ are all equivalent.

Counterexample: To prove that a statement of the form $\forall x P(x)$ is false, we need to find an x for which $P(x)$ is false. This x will be called counterexample for the statement $\forall x P(x)$.

Example: Every positive integer is sum of two squares.

3 cannot be written as sum of two squares.

Exhaustive Proof and Proof by cases: Sometime a theorem cannot be proved using a single arguments that holds for all possible cases. In this situation we consider different cases separately. This method is based on the following rule of inference; To prove a conditional statement of the form $(P_1 \vee P_2 \vee \cdots, P_n) \to Q$ we use the equivalence $(P_1 \vee P_2 \vee \cdots, P_n) \to Q \iff (P_1 \to Q) \wedge (P_2 \to Q) \wedge \cdots \wedge (P_n \to Q)$ can be used. This means that to prove the original condition statement where hypotheses is made up of a disjunction of $P_1, P_2, \cdots, P_n$ one has tp prove each conditional $P_i \to Q$ individually. This argument is called proof by case.

Sometime to prove a condition statement $P \to Q$ is true, it is helpful to consider the disjunction $P_1 \vee P_2 \vee \cdots \vee P_n$ instead of P as hypotheses, where $P \iff P_1 \vee P_2 \vee \cdots \vee P_n$.

Some theorems are proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs because these proofs proceed by exhausting all possibilities.

Without Loss of Generality: To reduce the number of cases WLOG is used where remaining cases can be proved by using the same argument.

Existence Proof: There are many theorems which assert that a particular type of object exists. i.e. the proposition of the form $\exists x P(x)$, where P is a predicate. A proof of the proposition $\exists x P(x)$ is called existence proof.

Sometime existence proof is given by finding an element α for which $P(\alpha)$ is true. Such existence proof is called constructive proof. Sometime, a nonconstructive proof of a proposition $\exists x P(x)$ can be given. That is we do not construct a particular element α satisfying $P(\alpha)$ but rather prove that $\exists x P(x)$ is true in some other way. For this purpose, we usually use the method of proof by contradiction.

Example: Show that there exists a positive integer that can be written as the sum of cubes of positive integers in two different ways.

$$1729 = 10^3 + 9^3 = 12^3 + 1^3,$$

this number is called **taxicab** number.

Nonconstructive proof: Show that there exists irrational numbers x and y such that x^y is rational.

$\sqrt{2}$ is known to be irrational. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we are done. If $\sqrt{2}^{\sqrt{2}}$ is irrational then let $x = \sqrt{2}^{\sqrt{2}}$, and $y = \sqrt{2}$ and we have

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2.$$

This we did not give a pair of irrational x, y such that x^y is rational but proved that one of the pairs $\sqrt{2}, \sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}, \sqrt{2}$ will serve the purpose.

Uniqueness Proofs: Some theorem asserts the existence of element with a particular property. In other words the assertion of the type "There is exactly one element with this property." To prove such theorems we prove two things;

Existence: Such an element x exists.
Uniqueness: If $y \neq x$, then y does not have this property.

Example: If a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

- **Set Theory (Equivalence relation, POSET, Induction, Zorn's Lemma)**
- **Lattices**
- **Boolean Algebra**
- **Recursion, Counting**
- **Graph (if time permits)**