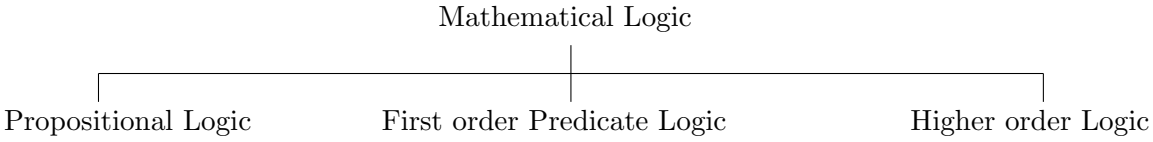
Discrete Mathematics 28/01/2019

Lecture 4: Mathematical Logic and Proof Techniques

Instructor: Goutam Paul *Scribe: Bhaskar Ray*

4.1 Mathematical Logic

Mathematical Logic can be broadly categorized into the following:



4.1.1 Propositional Logic

Definition 4.1. *A sentence which is either true or false is called a* ***proposition****.*

Definition 4.2. *A proposition which is always true is called a* ***tautology*** *and one which is always false is called a* ***contradiction****.*

Definition 4.3. *Two statements p and q are called* ***logically equivalent*** *if they have the same truth value i.e., p is true whenever q is true and p is false whenever q is false.*
If two statements p and q are logically equivalent, it is expressed as $p = q$ or $p \equiv q$.

Two or more propositions can be combined to form a new proposition using certain logical operators. Some common logical operators and their truth tables have been listed below.

Operator	Symbol
Negation	$\sim$
And	$\wedge$
Or	$\vee$
Implies	$\rightarrow$
Implies and is implied by	$\leftrightarrow$

p	q	$\sim p$	$\sim q$	$p \wedge q$	$p \vee q$	$p \rightarrow q$ $\equiv$ $\sim p \vee q$ $\equiv$ $\sim q \rightarrow \sim p$	$q \rightarrow p$ $\equiv$ $\sim q \vee p$ $\equiv$ $\sim p \rightarrow \sim q$	$p \leftrightarrow q$ $\equiv$ $(p \rightarrow q) \wedge (q \rightarrow p)$ $\equiv$ $\sim p \leftrightarrow \sim q$
F	F	T	T	F	F	T	T	T
F	T	T	F	F	T	T	F	F
T	F	F	T	F	T	F	T	F
T	T	F	F	T	T	T	T	T

We may observe that one can come up with tautologies and contradictions using these operators. For example, the statement $(p \leftrightarrow q) \leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$ is a tautology while $\sim p \wedge p$ is a contradiction.

Result 4.4. $\sim (\sim p) \equiv p$

Result 4.5 (De Morgan's Laws of Logic)**.** *As in the case for set theory, we have almost equivalent De-Morgan's laws for logical operators.*

i) $\sim (p \vee q) \equiv \sim p \wedge \sim q$

ii) $\sim (p \wedge q) \equiv \sim p \vee \sim q$

4.1.2 First Order Predicate Logic

A major drawback of *Propositional Logic* is that given a proposition, we cannot decide whether it is true or false. To counter the drawback, we introduce *First Order Predicate Logic*. We consider the following sentence:

Ron plays football

From our basic sense of English grammar, we identify that *Ron* is the subject here and *plays football* is the predicate, which refers to a property of the subject. We can now represent the sentence as $P(x)$, where P denotes the predicate *plays football* and x is the variable. Once a value (here it refers to a person) has been assigned to the variable x, the statement $P(x)$ becomes a proposition and has a certain truth value.

Remark 4.6. *The statement $P(x)$ is also said to be the value of the propositional function at x.*

For example, suppose we know that only Ron and Joe play football. Hence, the truth value of $P(Danny)$ will be *False* as the list of those who play football does not include Danny.

Definition 4.7. *A statement is **logically valid** if it is true in all interpretations.*

Remark 4.8. *With the additions of some extra axioms to **FOPL**, we get **First Order Theory***

4.1.3 Second Order Predicate Logic

We consider the same sentence as in the previous section. We can now include *football* in the subject and form a proposition $Q(x, y) = x\ plays\ y$. The predicate here, defines a relation between x and y as *who plays what*.
Suppose we come to know in addition that Ron and Joe do not play basketball and Danny plays only cricket. Then, the truth values of $Q(Danny, cricket)$, $Q(Joe, football)$ will be *True* while that of $Q(Ron, basketball)$ will be *False*.
In the same way, we can extend to *Higher Order Predicate Logic*.

4.1.4 Logical Theory

Predicate Logic along with some additional axioms form a *logical theory*. Some properties of interest for a logical theory are defined below:

1 **Completeness**: A logical theory is called *complete* if every true statement is provable[1].

2 **Soundness**: A logical theory is *sound* if anything that is provable in the theory is a true statement.

3 **Consistency**: A logical theory is *consistent* if $\nexists$ a well-formed formula wff^* such that both wff^* and $\sim wff^*$ are provable in the theory.

4 **Decidability**: A logical theory is *decidable* if it can be decided in polynomial order of time whether a well-formed formula is provable.

	Complete	Sound	Consistent	Decidable
Propositional Logic	Y	Y	?	Y
FOPL	Y	Y	?	N
Piano's Axiom of Arithmetic	N	Y	?	N

We now state two theorem related to completeness of a logical theory that addresses the question marks in the table.

Theorem 4.9 (Gödel's First Incompleteness Theorem)**.** *Any consistent extension, P of Piano's Arithmetic is incomplete i.e., there are true statements in the language of P which cannot be proved in P.*

Theorem 4.10 (Gödel's Second Incompleteness Theorem)**.** *If P is an extension of Piano's Arithmetic, consistency of P cannot be proved in P.*

For example, we need *Zermelo-Fraenkel set theory* and *Axiom of Choice* additionally to prove consistency of *FOPL*. Similarly, any extension of Piano's Arithmetic can be proved to be consistent by extending it further and using axioms from the extended theory.

4.2 Proof Techniques

Some basic and common techniques to prove a statement in a theory are listed below:

1 **Direct/Constructive Proof**: In this, to prove $p \rightarrow q$ we construct a sequence of *wff*'s following from p and each *wff*, along with the axioms implying the subsequent *wff* and ultimately implying a *wff* that is equivalent to q.

[1] A statement S is **provable** in a logical theory if there is a sequence of well-formed formulae $wff_1, wff_2, \ldots, wff_n$ such that wff_1 to wff_i follow from the axioms, rules of inference on wff_1 to wff_k along with the axioms yield wff_{k+1}, $i \leq k \leq n-1$ and $wff_n \equiv S$

The proofs of Theorem 4.9 and 4.10 have been omitted as these are beyond the scope of this discussion.

Example 4.11. *If p and q are distinct primes, show that $p^{q-1} + q^{p-1} \equiv 1(mod\ pq)$*
Solution: Using Euler's theorem, we have

$$q^{p-1} \equiv 1(mod\ p) \tag{1}$$
$$p^{q-1} \equiv 1(mod\ q) \tag{2}$$

since $gcd(p, q) = 1$.
From (1), we get

$$\implies \quad p|q^{p-1} - 1$$
$$p|q^{p-1} + p^{q-1} - 1$$

From (2), similarly, we obtain that

$$q|q^{p-1} + p^{q-1} - 1$$

Since p and q are distinct primes, we conclude that

$$pq|p^{q-1} + q^{p-1} - 1$$

which is equivalent to

$$p^{q-1} + q^{p-1} \equiv 1(mod\ pq)$$

2 **Proof by Cases**: To prove $p \to q$, where $p = p_1 \vee p_2 \vee \cdots \vee p_k$; we show that $p_i \to q \quad \forall \quad i = 1, 2, \ldots, k$.
We can justify it as follows:

$$\begin{aligned}(p_1 \vee p_2 \vee \cdots \vee p_k) \to q &\equiv \sim (p_1 \vee p_2 \vee \cdots \vee p_k) \vee q \\ &\equiv (\sim p_1 \wedge \sim p_2 \wedge \cdots \wedge \sim p_k) \vee q && [by\ De\ Morgan's] \\ &\equiv (\sim p_1 \vee q) \wedge (\sim p_2 \vee q) \wedge \cdots \wedge (\sim p_k \vee q) && [distibuting\ \vee\ over\ \wedge] \\ &\equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \cdots \wedge (p_k \to q)\end{aligned}$$

Thus, we have k cases to prove separately.

Example 4.12. *Prove that the square of any integer is of the form $4k$ or $4k + 1$ for some $k \in \mathbb{Z}$*
Solution: From division algorithm, we claim that for any integer n, we can represent n as $2m$ or $2m + 1$, for some $m \in \mathbb{Z}$
Case I: $n = 2m,\ m \in \mathbb{Z}$

$$\begin{aligned}n^2 &= (2m)^2 \\ &= 4m^2 \\ &\equiv 4k && [k = m^2]\end{aligned}$$

Case I: $n = 2m + 1,\ m \in \mathbb{Z}$

$$\begin{aligned}n^2 &= (2m + 1)^2 \\ &= 4m^2 + 4m + 1 \\ &\equiv 4k + 1 && [k = m^2 + m]\end{aligned}$$

Hence, combining the two cases, we get that the square of any integer is of the form $4k$ or $4k+1$ for some $k \in \mathbb{Z}$
Also refer to Example 4.14.

3 **Proof by Contrapositive**: We have seen earlier that $p \to q \equiv \sim q \to \sim p$. Thus, we form a constructive proof for $\sim q \to \sim p$ and use it to argue $p \to q$.

Example 4.13. *A, B, C are subsets of a universal set U. Prove that*

$$(A - C) \cap B \neq \phi \implies A \cap B \nsubseteq C$$

, where "-" denotes subtraction of sets.
Solution: We take the contrapositive of the statement, which is

$$A \cap B \subseteq C \implies (A - C) \cap B = \phi$$

We assume that LHS is true. Hence, we have

$$\forall x \in A \text{ and } x \in B,\ x \in C$$

Therefore, for $x \in (A - C)$,

$$\begin{aligned} & x \in A, x \notin C \\ \implies & x \notin B && [since,\ if\ x \in B, x \in A \cap B \implies x \in C] \\ \implies & (A - C) \cap B = \phi \end{aligned}$$

Hence, the statement in the question is true.

4 **Proof by Contradiction**: We have seen from the truth table that

$$p \to q \equiv \sim p \vee q$$

. Therefore,

$$\begin{aligned} & p \to q = T \\ \Leftrightarrow \quad & \sim p \vee q = T \\ \Leftrightarrow \quad & \sim (\sim p \vee q) = F \\ \Leftrightarrow \quad & p \wedge \sim q = F && [De\ Morgan's] \end{aligned}$$

We thus constructively prove that $p \wedge \sim q$ leads to a contradiction and hence, argue that $p \to q$.

Example 4.14. *For a prime p such that $p \equiv 3 \pmod 4$, prove that $\nexists\ x \in \mathbb{Z}$ s.t. $x^2 \equiv -1 \pmod p$.*
Solution: For the sake of contradiction, let us assume that for $p \equiv 3 \pmod 4$, $\exists\ x \in \mathbb{Z}$ s.t. $x^2 \equiv -1 \pmod p$. Then,

$$(x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod p$$

. *Since* $p \equiv 3 \ (mod\ 4)$, $\frac{p-1}{2}$ *is odd. Therefore,*

$$x^{p-1} \equiv -1 \ (mod\ p)$$

Case I: $p|x$
Clearly, $p|x^{p-1}$ *as* $p > 2$*. Hence, our assumption is false.*
Case II: $p \nmid x$
As p *is prime,* $gcd(x, p) = 1$*. This in turn, implies that*

$$x^{p-1} \equiv 1 \ (mod\ p)$$

Combining it with our assumption, we obtain $p|2$ *which implies* $p = 2$*.*
This cannot be true as $p \equiv 3 \ (mod\ 4)$*.*
Hence, we obtain a contradiction in each of the cases. Thus we claim that our assumption is false, which means that the statement in the question is true.

5 **Proof by Induction**: In this technique, we use *Principle of Weak Induction (WIP)* or *Principle of Strong Induction (SIP)* as discussed in Lecture 3.

Example 4.15 (Fermat's theorem)**.** *Let* p *be a prime and* a *be any integer. Then prove that* $a^p \equiv a \ (mod\ p)$
Solution by Induction on a*: First, we prove the theorem for all positive integers. For the base case, the statement is trivially true for* $a = 1$*.*
Induction hypothesis: *Assume that statement is true for some* $a \geq 1$ *i.e.,*

$$a^p \equiv a \ (mod\ p)$$

Using binomial theorem, we have

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1$$

We observe that since p *is a prime,* $p|p!$ *and* $p \nmid k! \ \forall \ k = 1, 2, \ldots, p-1$*.*
Hence, $p|\binom{p}{k} \ \forall \ k = 1, 2, \ldots, p-1$*. Thus, the middle terms vanish modulo* p*. Therefore,*

$$\begin{aligned}(a+1)^p &\equiv (a^p + 1) \ (mod\ p) \\ &\equiv (a+1) \ (mod\ p) \qquad\qquad [by\ induction\ hypothesis]\end{aligned}$$

Hence, the statement is true for $a + 1$*.*
Therefore, by Principle of Mathematical Induction, we conclude that the statement is true $\forall \ a \geq 1$*.*
Now, the statement is trivially true for $a = 0$*. Also, every negative integer is congruent to some positive integer modulo* p*. Thus, the theorem holds for all* $a \in \mathbb{Z}$*.*