CS34110 Discrete Mathematics and Graph Theory

UNIT – I, Module – 2

Lecture 07: Predicate logic

[Theorem, proof, axiom, lemma, conjecture; Proof method; Direct, vacuous, trivial proofs; Proofs by contraposition, contradiction]

Dr. Suddhasil De

Proof logic: Terminologies

- Theorem: important mathematical or logical statement, proven to be TRUE.
  - Theorem also sometimes referred as: proposition or fact or result.
- Proof: valid argument, establishing truth of theorem.
  - Constituents/ingredients of proof: (i) premises/hypotheses of theorem, if any, to be proven; (ii) axioms assumed to be true; (iii) previously proven theorems; (iv) rules of inference to be applied.
- Axiom (or postulate): statement stated using primitive terms, and assumed to be TRUE.

Proof logic: Terminologies

- Informal proof: proof designed for human consumption, where multiple rules of inference used in each step without explicitly stated, steps skipped, axioms being assumed etc.
  - Informal proof → human interpretable, easy to follow. Formal proof → extremely long, hard to follow.
- Lemma (plural lemmas or lemmata): intermediate result, also proven to be TRUE, and helpful in proof of important theorem.
  - Complicated proof of theorem → proven using series of lemmas for easier understanding, where each lemma to be proved individually.

Proof logic: Terminologies

- Corollary: theorem, established directly from another theorem already proven.
- Conjecture: statement being proposed to be TRUE statement, usually on basis of some partial evidence, heuristic argument, or intuition of expert.
  - Conjecture $\xrightarrow{\text{proven}}$ Theorem.

Proof methods

- Proof methods: methods to provide overall approach and strategy of proofs.
  - Types of proof methods: Direct Proof;
    Proof by Contraposition; Proof by Contradiction;
    Vacuous Proof; Trivial Proof;
    Proof of Equivalence; Proof by Cases; Proof by Exhaustion;
    Proof by Construction (types: proof by example, by counterexample);
    Nonconstructive Existence Proof;
    Uniqueness Proof;
    Proof by Mathematical Induction etc.

Proof methods

- Proof methods:
  - How to construct Proof:
    (i) choice of proof method;
    (ii) premises of theorem to be proven;
    (iii) axioms assumed to be true;
    (iv) previously proven theorems;
    (v) applying rules of inference successively.

Proof methods

- 'Direct proof' method: proof constructed by assuming hypothesis to be TRUE, and subsequent steps following rules of inference to use axioms, definitions, previously proven theorems, with final step showing conclusion to be TRUE.
  - Commonly followed to prove implication statements.

Proof methods

- 'Direct proof' method examples:
  - Example-1:: Proof for theorem "If n is an odd integer, then n^2 is odd."

    Proof: Denoting "n is an odd integer" as $P(n)$, "n^2 is odd" as $Q(n)$, $\forall n(P(n) \rightarrow Q(n))$ express given theorem in domain of discourse $= \mathbb{Z}$.

    Plan: to show first $P(c) \rightarrow Q(c)$ as TRUE, (where c = arbitrary integer and $c \in \mathbb{Z}$), and then to apply universal generalization.

    $P(c) \rightarrow Q(c)$ to be TRUE, unless $P(c) \equiv$ TRUE but $Q(c) \equiv$ FALSE, as per definition of implication.

    First, assume $P(c) \equiv$ TRUE, i.e., "c is odd integer"; so as per definition of odd number, $c = 2k + 1$, for some integer $k \in \mathbb{Z}$.

(contd. to next slide)

Proof methods

- 'Direct proof' method examples:
  - Example-1 (contd.)::

    Squaring both sides of equation in last slide, $c^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

    Denoting $2k^2 + 2k = k'$, where $k' \in \mathbb{Z}$, $c^2 = 2k' + 1$., i.e., as per definition of odd number, "c^2 is odd", so $Q(c) \equiv$ TRUE.

    So, $P(c) \rightarrow Q(c) \equiv$ TRUE for arbitrary c.

    Applying universal generalization as per (II.8), $\forall n(P(n) \rightarrow Q(n)) \equiv$ TRUE. ■

Proof methods

- 'Proof by contraposition' method: proof constructed based on contrapositive property of implication, in which assuming negation of conclusion as TRUE, and subsequent steps following rules of inference to use axioms, definitions, previously proven theorems, with final step showing negation of hypothesis to be TRUE.
  - Also commonly followed to prove implication statements.
- ➲ Note: when TRUE hypothesis not leading to TRUE conclusion by 'direct proof', then to apply 'proof by contraposition' → 'direct proof' to show FALSE conclusion leading to FALSE hypothesis.

Proof methods

- 'Proof by contraposition' method:
  - One form of 'Indirect proof' method, due to not possible to apply 'direct proof' method on implication statement.

Proof methods

- 'Proof by contraposition' method examples:
  - Example-1:: Proof for theorem "If n is an integer and $3n + 2$ is odd, then n is odd."

  Proof: Denoting "$3n + 2$ is odd" as $R(n)$, "n is odd" as $S(n)$, $\forall n(R(n) \rightarrow S(n))$ express given theorem in domain of discourse $= \mathbb{Z}$. No straightforward 'direct proof' to conclusively prove given theorem. Plan: to show first $\neg S(a) \rightarrow \neg R(a)$ as TRUE, (where a = arbitrary integer and $a \in \mathbb{Z}$), next to apply (I.14) rule, and then to apply universal generalization.
  First, assume $\neg S(a) \equiv$ TRUE, i.e. "a is even."

(contd. to next slide)

Proof methods

- 'Proof by contraposition' method examples:
  - Example-1 (contd.)::
    So as per definition of even number, $a = 2k$, for some integer k.
    Substituting $2k$ for a, $3a + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$.
    Denoting $3k + 1 = k''$, where $k'' \in \mathbb{Z}$, $3a + 2 = 2k''$; i.e., as per definition of even number, "$3a + 2$ is even", so $\neg R(a) \equiv$ TRUE.
    So, $\neg S(a) \rightarrow \neg R(a) \equiv$ TRUE for arbitrary a.
    Applying (I.14), $R(a) \rightarrow S(a) \equiv$ TRUE for arbitrary a.
    Applying universal generalization as per (II.8) on above,
    $\forall n(R(n) \rightarrow S(n)) \equiv$ TRUE. ■

Proof methods

- 'Proof by contradiction' method: proof constructed assuming negation of hypothesis as antecedent of implication with value FALSE, introducing new (but related) consequent of implication with value TRUE, and subsequent steps following rules of inference to use axioms, definitions, previously proven theorems, with final step showing new consequent to be FALSE (i.e., consequent to become FALSE due to contradiction law).
  - Typical form of 'contradictory' consequent introduced: $(q \wedge \neg q)$, such that $\neg p \rightarrow \neg(q \wedge \neg q)$ to be come TRUE (p to be theorem statement).
    As $\neg(q \wedge \neg q)$ FALSE, so $\neg p$ to be FALSE, and then p to be TRUE.

Proof methods

- 'Proof by contradiction' method:
  - Another form of 'Indirect proof' method, due to not possible to apply 'direct proof' method to prove hypothesis statement.
  - Also used to prove theorem of conditional statements;
    strategy: to assume negation of conclusion to be TRUE → to conjunct premises of given theorem and negation of conclusion → to follow rules of inference, axioms, definitions, previously proven theorems in order to arrive at contradiction, i.e., $(p \wedge \neg q) \rightarrow \mathrm{F} \equiv p \rightarrow q$.

Proof methods

- 'Proof by contradiction' method examples:
  - Example-1:: Proof for theorem "$\sqrt{2}$ is irrational."

  Proof: Denoting hypothesis as p: "$\sqrt{2}$ is irrational," so $\neg p \equiv$ "It is not case that $\sqrt{2}$ is irrational" $\equiv$ "$\sqrt{2}$ is rational."
  No straightforward 'direct proof' to conclusively prove given theorem.
  Plan: assuming $\neg p$ as TRUE, to show $\neg p \rightarrow \neg(q \wedge \neg q)$ becoming TRUE, where q to choose judiciously and relevant to p.
  $\neg p \equiv$ TRUE $\equiv$ "$\sqrt{2}$ is rational"; $\therefore \sqrt{2}$ representable as: $\sqrt{2} = \frac{a}{b}$, $b \neq 0$, and no common factors in a and b (i.e., a/b in lowest terms).

(contd. to next slide)

Proof methods

- 'Proof by contradiction' method examples:
  - Example-1 (contd.)::
    Squaring, $2 = \frac{a^2}{b^2}$. $\therefore 2b^2 = a^2$. So, as per definition of even number, $a^2 =$ even integer.
    As per established theorem: "If m and n are integers and mn is even, then m is even or n is even," $a =$ even integer $= 2c$ for some integer c. So, $2b^2 = 4c^2$. $\therefore b^2 = 2c^2$. So, $b^2 =$ even integer, i.e., $b =$ even.
    So, both a and b even integers, i.e., a and b have common factor 2.
    So, let $q \equiv$ "2 is not common factor between a and b."
    Then, $\neg q \equiv$ "2 is common factor between a and b."

(contd. to next slide)

Proof methods

- 'Proof by contradiction' method examples:
  - Example-1 (contd-2.)::
    Consequently, starting with assumption $\neg p$ as TRUE leading to equation $\sqrt{2} = \frac{a}{b}$, $b \neq 0$, with q judiciously chosen to be TRUE, but simplifying same equation leading to $\neg q$ also to become TRUE.
    So, $\neg(q \wedge \neg q) =$ FALSE, by contradiction law, and $\neg p \rightarrow \neg(q \wedge \neg q)$.
    Because assuming $\neg p$ leading to FALSE proposition: "2 divides both a and b" and "2 does not divide both a and b",
    so $\neg p$ must be FALSE.
    $\therefore p \equiv$ "$\sqrt{2}$ is irrational" $\equiv$ TRUE. ■

Proof methods

- 'Vacuous Proof' method: proof constructed by only showing antecedent of implication to be FALSE (following rules of inference to use axioms, definitions, previously proven theorems), with final step concluding implication to be TRUE.
  - Often used to establish special cases of theorems based on implication statement.
  - ➲ Note: 'Vacuous' effect of consequent in truth value of implication.

Proof methods

- 'Vacuous Proof' method examples:
  - Example-1:: Proof of proposition $P(0)$ to be TRUE, where $P(n)$ be "If $n > 1$, then $n^2 > n$" and domain of discourse of all integers.

  Proof: Expressing $P(0)$: "If $0 > 1$, then $0^2 > 0$."
  Antecedent of $P(0)$ becoming FALSE, as $0 \not> 1$.
  So, Antecedent → Consequent ≡ TRUE, due to Antecedent ≡ FALSE, as per definition of implication.
  Thus, $P(0) \equiv$ TRUE. ■
  - ➲ Note: in example-1, consequent of $P(0)$, i.e., $0^2 > 0 \equiv$ FALSE, irrelevant to truth value of $P(0)$, when antecedent of $P(0) \equiv$ FALSE.

Proof methods

- 'Trivial Proof' method: proof constructed by only showing consequent of implication to be TRUE (following rules of inference to use axioms, definitions, previously proven theorems), with final step concluding implication to be TRUE.
  - Also often used to establish special cases of theorems based on implication statement.
  - ➲ Note: No effect (or no need) of antecedent in truth value of implication.

Proof methods

- 'Trivial Proof' method examples:
  - Example-1:: Proof of proposition $P(0)$ to be TRUE, where $P(n)$ be "If a and b be positive integers with $a \geq b$, then $a^n \geq b^n$," and domain of discourse consisting of all nonnegative integers.

  Proof: Expressing $P(0)$: "If $a \geq b$, then $a^0 \geq b^0$."
  Consequent of $P(0)$ becoming TRUE, as $a^0 = b^0 = 1$.
  So, Antecedent → Consequent ≡ TRUE, due to Consequent ≡ TRUE, as per definition of implication.
  Thus, $P(0) \equiv$ TRUE. ■
  - ➲ Note: in example-1, antecedent of $P(0)$, i.e., $a \geq b$, not needed.

Summary

- Focus: Predicate logic (contd.).
- Theorem, Proof, Axiom, Lemma, Corollary, Conjecture definitions.
- Proof method definition and types.
- Direct proof method definition and examples.
- Proof by contraposition method definition and examples.
- Proof by contradiction method definition and examples.
- Vacuous proof method definition and examples.
- Trivial proof method definition and examples.

References

1. [Ros21] Kenneth H. Rosen, Kamala Krithivasan, *Discrete Mathematics and its Applications*, Eighth edition, McGraw-Hill Education, 2021.
2. [Ross12] Kenneth A. Ross, Charles R. B. Wright, *Discrete Mathematics*, Fifth edition, Pearson Education, 2012.
3. [Mot15] Joe L. Mott, Abraham Kandel, Theodore P. Baker, *Discrete Mathematics for Computer Scientists and Mathematicians*, Second edition, Pearson Education, 2015.
4. [Lip07] Seymour Lipschutz, Marc L. Lipson, *Schaum's Outline of Theory and Problems of Discrete Mathematics*, Third edition, McGraw-Hill Education, 2007.

Further Reading

- Proof terminologies:: [Ros21]:84-85.
- Proof method:: [Ros21]:86.
- Direct proof:: [Ros21]:86-87,89-90.
- Proof by contraposition:: [Ros21]:87-88,89-90.
- Proof by contradiction:: [Ros21]:90-92.
- Vacuous proof:: [Ros21]:88-89.
- Trivial proof:: [Ros21]:88-89.

Lecture Exercises: Problem 1

Proof of "Fundamental theorem of arithmetic" (also called "unique factorization theorem" or "prime factorization theorem"):

Every integer (>1) can be represented uniquely as product of prime numbers, up to order of factors (i.e., ignoring other reorder of factors).

Or,

Every integer (>1), is either prime, or unique product of primes.

Mathematically, every $n \in \mathbb{Z}$ and $n > 1$ represented in exactly one way as product of prime powers: $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_k}^{\alpha_k} = \prod_{i=1}^{k} {p_i}^{\alpha_i}$, where primes $p_1 < p_2 < \cdots < p_k$, and $\alpha_1, \alpha_2, \ldots, \alpha_k$ their associated positive integer powers.