CSL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Rules of Inference for Quantified Statements

Rule of inference	Name
$\forall x\ P(x)$ $\therefore ?$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore ?$	Universal generalization
$\exists x\ P(x)$ $\therefore ?$	Existential instantiation
$P(c)$ for some element c $\therefore ?$	Existential generalization
$\forall x(P(x) \rightarrow Q(x))$ $P(a)$ where a is a particular element in the domain $\therefore ?$	Universal modus ponens
$\forall x(P(x) \rightarrow Q(x))$ $\neg Q(a)$ where a is a particular element in the domain $\therefore ?$	Universal modus tollens

Table: Rules of inference for quantified statements

Rule of inference	Name
$\forall x\ P(x)$ / $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c / $\therefore \forall x\ P(x)$	Universal generalization
$\exists x\ P(x)$ / $\therefore P(x)$ for some element c	Existential instantiation
$P(c)$ for some element c / $\therefore \exists x\ P(x)$	Existential generalization
$\forall x(P(x) \rightarrow Q(x))$, $P(a)$ where a is a particular element in the domain / $\therefore Q(a)$	Universal modus ponens
$\forall x(P(x) \rightarrow Q(x))$, $\neg Q(a)$ where a is a particular element in the domain / $\therefore \neg P(a)$	Universal modus tollens

Table: Rules of inference for quantified statements

- Use rules of inference for quantified statements to show 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 has passed the first exam has not read the book.*"

Proofs

- Theorem: A mathematical statement that can be shown to be true.
  - Theorem is usually reserved for a statement that is considered at least somewhat important.
  - Less important theorems sometimes are called *propositions*.
- Axiom (or postulate): A statement that is assumed to be true.
- Lemma: A less important theorem that is helpful in the proof of other results.
- Corollary: A theorem that can be established directly from a theorem that has been proved.
- Conjecture: A statement that is being proposed to be a true statement, usually on the basis of some partial evidence.

- Theorem: A mathematical statement that can be shown to be true.
  - Theorem is usually reserved for a statement that is considered at least somewhat important.
  - Less important theorems sometimes are called *propositions*.
- Axiom (or postulate): A statement that is assumed to be true.
- Lemma: A less important theorem that is helpful in the proof of other results.
- Corollary: A theorem that can be established directly from a theorem that has been proved.
- Conjecture: A statement that is being proposed to be a true statement, usually on the basis of some partial evidence.
- Proof: A valid argument that establishes the truth of a Theorem.
  - The statements used in a proof can include axioms, definitions, the premises, if any, of the theorem, and previously proven theorems and uses rules of inference to draw conclusions.

- Direct proof: Used for showing statements of the form $p \rightarrow q$. We assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.
- Example: Give a direct proof of the theorem "*if n is an odd integer, then n^2 is odd*."

Definition (Even and odd)

The integer n is even if there exists an integer k such that $n = 2k$, and n is odd is there exists an integer such that $n = 2k + 1$.

- Proof by contraposition: Used for proving statements of the form $p \rightarrow q$. We take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow.
- Examples:
  - Prove that if n is an integer and $3n + 2$ is odd, then n is odd.
  - Prove that if n is an integer and n^2 is odd, then n is odd.
  - Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

- Vacuous proof: When proving $p \to q$, a proof showing p to be false is called a vacuous proof.
  - Example: Show that the proposition $P(0)$ is true, where $P(n)$ is "if $n > 1$, then $n^2 > n$" and the domain consists of all integers.
- Trivial proof: When proving $p \to q$, a proof showing q to be true is called a trivial proof.
  - Example: Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

- Direct proof
- Proof by contraposition
- Proof by contradiction: Suppose we want to prove that a statement p is true and suppose we can find a contradiction q such that $\neg p \to q$ is true. Since q is false, but $\neg p \to q$ is true, we can conclude that $\neg p$ is false, which means that p is true. The contradiction q is usually of the form $r \wedge \neg r$ for some proposition r.
- Examples:
  - Show that at least four of any 22 days must fall on the same day of the week.

- Direct proof
- Proof by contraposition
- Proof by contradiction: Suppose we want to prove that a statement p is true and suppose we can find a contradiction q such that $\neg p \rightarrow q$ is true. Since q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true. The contradiction q is usually of the form $r \wedge \neg r$ for some proposition r.
- Examples:
  - Show that at least four of any 22 days must fall on the same day of the week.
  - Prove that $\sqrt{2}$ is irrational by giving proof by contradiction.

Definition (Rational and irrational)

The real number r is rational if there exists integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called irrational.

- Direct proof
- Proof by contraposition
- Proof by contradiction: Suppose we want to prove that a statement q is true and suppose we can find a contradiction t such that $\neg q \rightarrow t$ is true. Since t is false, but $\neg q \rightarrow t$ is true, we can conclude that $\neg q$ is false, which means that q is true. The contradiction t is usually of the form $r \wedge \neg r$ for some proposition r.
- Proof by contraposition is a special case of proof by contradiction.
  - We assume that the premise p is true. Then we show that $\neg q \rightarrow \neg p$. Now since $[(\neg q \rightarrow \neg p) \wedge p] \rightarrow [\neg q \rightarrow (p \wedge \neg p)]$ is a tautology, we conclude $\neg q \rightarrow (p \wedge \neg p)$ which implies that q is true.

- Direct proof
- Proof by contraposition
- Proof by contradiction: Suppose we want to prove that a statement q is true and suppose we can find a contradiction t such that $\neg q \rightarrow t$ is true. Since t is false, but $\neg q \rightarrow t$ is true, we can conclude that $\neg q$ is false, which means that q is true. The contradiction t is usually of the form $r \wedge \neg r$ for some proposition r.
- Examples:
  - Show that at least four of any 22 days must fall on the same day of the week.

- Direct proof
- Proof by contraposition
- Proof by contradiction: Suppose we want to prove that a statement q is true and suppose we can find a contradiction t such that $\neg q \rightarrow t$ is true. Since t is false, but $\neg q \rightarrow t$ is true, we can conclude that $\neg q$ is false, which means that q is true. The contradiction t is usually of the form $r \wedge \neg r$ for some proposition r.
- Examples:
  - Show that at least four of any 22 days must fall on the same day of the week.
  - Prove that $\sqrt{2}$ is irrational by giving proof by contradiction.

Definition (Rational and irrational)

The real number r is rational if there exists integers p and q with $q \neq 0$ such that $r = p/q$. A real number that is not rational is called irrational.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Other ideas:
  - Proofs of equivalence:
    - To show statements of the form $p \leftrightarrow q$ we have to show $p \rightarrow q$ and $q \rightarrow p$.
    - How do we show $p_1 \leftrightarrow p_2 \leftrightarrow ... \leftrightarrow p_n$?

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Other ideas:
  - Proofs of equivalence:
    - To show statements of the form $p \leftrightarrow q$ we have to show $p \rightarrow q$ and $q \rightarrow p$.
    - To show $p_1 \leftrightarrow p_2 \leftrightarrow ... \leftrightarrow p_n$, it is sufficient to show that $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, ..., $p_{n-1} \rightarrow p_n$, $p_n \rightarrow p1$
    - Example: Show that the following statements are equivalent: (p_1) n is even, (p_2) $n - 1$ is odd, (p_3) n^2 is even.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Other ideas:
  - Proofs of equivalence
  - Proof by counterexample: Suppose we want to show that the statement $\forall x\ P(x)$ is false then we only need to find a counterexample, that is, an example x for which $P(x)$ is false.
    - Example: Show that the statement "Every positive integer is the sum of squares of two integers" is false.

- What is wrong with the following proofs?
  - "Theorem": If n^2 is positive, then n is positive.
    - "Proof": Suppose that n^2 is positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n is positive.
  - "Theorem": If n is not positive, then n^2 is not positive.
    - "Proof": Suppose that n is not positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n^2 is not positive.
  - "Theorem": If n^2 is even, then n is even.
    - "Proof": Suppose that n^2 is even. Then $n^2 = 2k$ for some integer k. Let $n = 2l$ for some integer l. This shows that n is even.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Proof by cases: Suppose we want to show a statement of the form $(p_1 \vee p_2 \vee ... \vee p_n) \rightarrow q$. That is, a statement where the hypothesis is made of a disjunction of propositions. Then such a statement can be proven by proving each of the n conditional statements $p_i \rightarrow q, i = 1, 2, ..., n$.
  - This follows from the tautology $[(p_1 \vee p_2 \vee ... \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge ... \wedge (p_n \rightarrow q)]$.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Proof by cases
- Exhaustive proofs (proofs by exhaustion): This is a special case of proof by cases where each case involves checking a single example.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Proof by cases
- Exhaustive proof (proof by exhaustion): This is a special case of proof by cases where each case involves checking a single example.
  - Prove that $(n+1)^3 \geq 3^n$, if n is a positive integer with $n \leq 4$.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases:
  - Prove that if n is an integer, then $n^2 \geq n$.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases:
  - Without loss of generality (WLOG): When the phrase "without loss of generality" is used in a proof, we assert that by proving one case of a theorem, no additional argument is required to prove other specified cases. That is, other cases follow by making straightforward changes to the argument, or by filling in some straightforward initial step.
  - Example: Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases:
  - What is wrong with this "proof"?
    "Theorem:" If x is a real number, then x^2 is a positive real number.
    "Proof:" Let p_1 be "x is positive," let p_2 be "x is negative," and let q be "x^2 is positive." To show that $p_1 \rightarrow q$ is true, note that when x is positive, x^2 is positive because it is the product of two positive numbers, x and x. To show that $p_2 \rightarrow q$, note that when x is negative, x^2 is positive because it is the product of two negative numbers, x and x. This completes the proof.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases
- Existence proofs: Used for propositions of the form $\exists x\ P(x)$.
  - Constructive proof: Find an element a (called a *witness*) such that $P(a)$ is true.
  - Nonconstructive proof: Proof without finding a witness. (Usually by contradiction.)

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases
- Existence proofs
  - Examples:
    - Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases
- Existence proofs
  - Examples:
    - Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.
    - Show that there exist irrational numbers x and y such that x^y is rational.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases
- Existence proofs
- Uniqueness proofs: Statements that assert the existence of a unique elements with a particular property. The two parts of a uniqueness proof are:
  - Existence: Show that an element x with desired property exists.
  - Uniqueness: Show that $y \neq x$, then y does not have the desired property.

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proofs of equivalence
- Proof by counterexample
- Exhaustive proof
- Proof by cases
- Existence proofs
- Uniqueness proofs
  - Example:
    - Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

End