COL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Proofs

- 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 $ar + b = 0$.

Proof Strategies

- Forward reasoning: Use the premises, axioms, previous theorems in a sequence of steps to show that the conclusion follows. This also includes indirect proofs.
  - Issue: We might not know which premise, axiom, or theorem to use to derive the relevant conclusion.
- Backward reasoning: For proving a statement q, we try to find a statement p such that p is true and $p \rightarrow q$.
  - Example: Show that $(x + y)/2 > \sqrt{xy}$ when x and y are distinct positive real numbers.

- Forward and backward reasoning
- Adapting existing proofs: Adapting an existing proof to prove other facts.
  - Example: Show that $\sqrt{3}$ is irrational.

- Forward and backward reasoning
- Adapting existing proofs
- Proof vs counterexample: For a new statement, switching back and forth between trying to prove the statement of finding a counterexample.
  - Example: Prove or disprove: "*Every positive integer is the sum of squares of three integers.*"

Definition (Graph)

A graph $G = (V, E)$ consists of V, a non-empty set of vertices (or nodes) and E, a set of edges. Each edge has two vertices associated with it, called its endpoints. An edge is said to connect its endpoints. The degree of a vertex is the number of edges incident on this vertex.

- Prove or disprove the following:
  - For any graph there are two vertices that have the same degree.
  - For any graph the number of odd degree vertices is even.

End