Discrete Math

11 – Proofs: Basics

Outline

- Terminology
- Proof Methods
- Incorrect Proofs

Terminology

- A *theorem* is a proposition that can be shown to be true.
- A *lemma* is a preliminary proposition useful for proving later propositions.
- A *corollary* is a proposition that can be established directly from a theorem.
- A *conjecture* is a proposition that is being proposed to be a true statement.

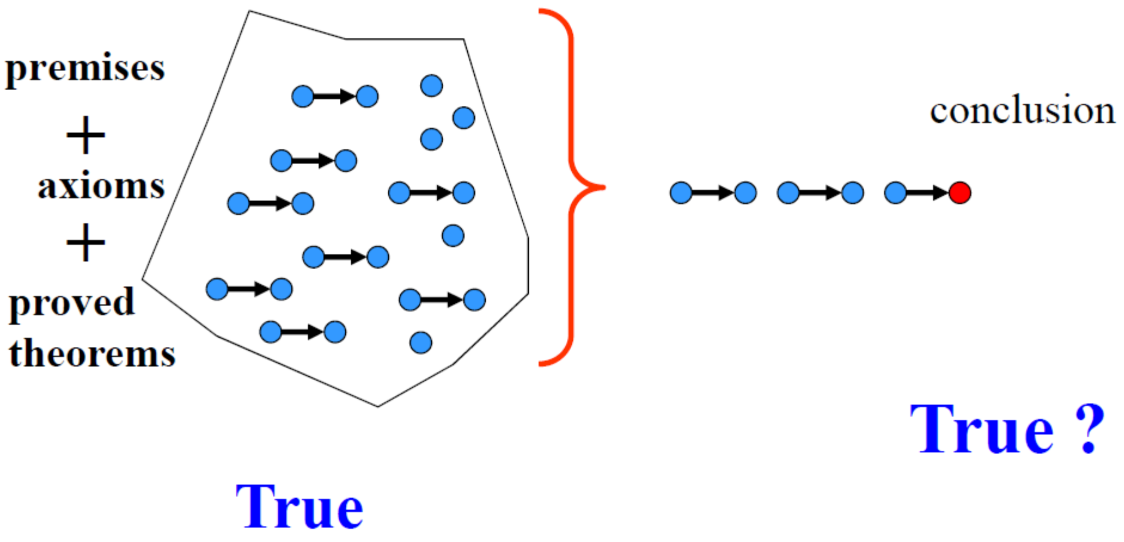
Terminology

Propositions that are simply accepted as true are called *axioms*.

- Examples:
  - For all real numbers x and y, $x + y = y + x$.
  - There is a straight-line segment between every pair of points.

Terminology

- A *proof* is a valid argument that establishes the truth of a statement.
  - can use axioms, premises (if any), and previously proved theorems.



Common Forms of Theorems

- T
- $\exists x\, T(x)$
- $\forall x\, T(x)$
  - Special cases of $T(x)$: $P(x) \longrightarrow Q(x)$ and $P \leftrightarrow Q$

Common Forms of Theorems

- T
  - Example: "$\sqrt{2}$ is not a rational number."
- $\exists x\ T(x)$
  - Example: "There exists one integer *n* such that $n^2 + n + 41$ is composite."
  - Find an element *a* in the domain such that T(*a*) is true and then apply Existential Generalization.
  - To disprove, prove that T(x) is false for all elements in the domain.

Common Forms of Theorems

- $\forall x\,(P(x) \longrightarrow Q(x))$
  - Example: “For any integer *n*, if 3*n*+2 is odd, then *n* is odd.”
  - Show that $P(c) \longrightarrow Q(c)$, where c is an arbitrary element of the domain, and then apply Universal Generalization.
  - Show that Q is true if P is true.
  - To disprove, find an element *e* such that P(*e*) is true, but Q(*e*) is false.
- $\forall x\,(P \leftrightarrow Q)$
  - Proving $P \leftrightarrow Q$ is equivalent to proving $(P \longrightarrow Q) \land (Q \longrightarrow P)$.

Proof Methods

- Direct Proof
- Proof by Contraposition
- Proof by Contradiction
- Proof by Cases

Direct Proof

- Directly show that if P is true, then Q must be true, using axioms, definitions, and previously proven theorems, together with inference rules.

Examples

1. Prove that "If n is odd, then n^2 is odd."

Proof:

- Assume that n is odd, then $n = 2k + 1$, where k is some integer.
- We have $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.
- Therefore, n^2 is an odd integer.

Examples

2. Prove that “If m and n are both perfect squares, then mn is also a perfect square.”

Proof:

- Assume that m and n are both perfect squares, then $m = s^2$ and $n = t^2$, where s and t are some integers.
- We have $mn = s^2t^2 = (st)^2$.
- Therefore, mn is a perfect square.

Exercise

Prove that “Every odd integer is the difference of two squares.”

Exercise

Prove that "Every odd integer is the difference of two squares."

Proof:

- Assume that n is odd, then $n = 2k + 1$, where k is some integer.
- $n = 2k + 1 = k^2 + 2k + 1 – k^2 = (k+1)^2 - k^2$.

Proof by Contraposition

Instead of proving $P \longrightarrow Q$, prove $\neg Q \longrightarrow \neg P$

Why?

Implication Law: $P \longrightarrow Q \equiv \neg Q \longrightarrow \neg P$

Examples

1. Prove that “For any integer n, if n^2 is even, then n is even.”

Proof:

- Contraposition: “If n is odd, then n^2 is odd.”
- Example 1 of Direct Proof.
- We have proved the theorem “For any integer n, if n^2 is even, then n is even.”

Examples

2. Prove that “If $3n + 2$ is odd for an integer n, then n is odd.”

Proof:

- Contraposition: “If n is even, then $3n + 2$ is even.”
- Assume that n is even, then $n = 2k$, where k is some integer.
- We have $3n + 2 = 6k + 2 = 2(3k + 1)$.
- Therefore $3n + 2$ is even.
- We have proved the theorem “If $3n + 2$ is odd, then n is odd.”

Examples

3. Prove that “If r is irrational, then $\sqrt{r}$ is also irrational.”

Proof:

- Contraposition: “if $\sqrt{r}$ is rational, then r is rational.”
- Assume that $\sqrt{r}$ is rational.
- There exist integers p and q (no common factors), such that $\sqrt{r} = \frac{p}{q}$.
- Squaring both sides gives: $r = \frac{p^2}{q^2}$.
- Since p^2 and q^2 are integers, r is also rational.
- This completes the proof.

Exercise

Prove that "If $x + y \geq 2$, where x and y are real numbers, then $x \geq 1$ or $y \geq 1$."

Exercise

Prove that "If $x + y \geq 2$, where x and y are real numbers, then $x \geq 1$ or $y \geq 1$."

Proof:

- Contraposition: "If $x < 1$ and $y < 1$, then $x + y < 2$."
- Since $x < 1$ and $y < 1$, we have $x + y < 2$.
- Therefore we have proved the theorem.

Proof by Contradiction

- Assume we want to prove S is true.
- Suppose we can find a contradiction C such that $\neg S \longrightarrow C$ is true.
- Since C is false, but $\neg S \longrightarrow C$ is true, then S must be true.

Example

Prove that "$\sqrt{2}$ is not a rational number."

Proof:

- Assume that $\sqrt{2}$ is a rational number.
- Then $\sqrt{2} = \frac{p}{q}$, where p and q have no common factors, and $2 = \frac{p^2}{q^2}$, or $2q^2 = p^2$.
- Since p^2 is even, p is even. (Example 1 of Proof by Contraposition)
- This means that 2 is a factor of p; hence 4 is a factor of p^2, and the equation $2q^2 = p^2$ can be written as $2q^2 = 4x$ or $q^2 = 2x$ for some integer *x*.
- We have q^2 is even and thus q is even. (Example 1 of Proof by Contraposition)
- Now 2 is a factor of *q* and a factor of *p*, which contradicts the statement that *p* and *q* have no common factors.
- Hence $\sqrt{2}$ is not rational.

Proof by Contradiction

Propositions of Implication Forms: $P \longrightarrow Q$

Instead of $P \longrightarrow Q$, prove $\neg(P \longrightarrow Q) \longrightarrow \mathbf{F}$ or $(P \land \neg Q) \longrightarrow \mathbf{F}$

How to find a contradiction?

- Imply Q. Then assert $Q \land \neg Q$ as a contradiction.
- Imply $\neg P$. Then assert $P \land \neg P$ as a contradiction.
- Imply $R \land \neg R$ during the proof for some proposition R.

Examples

1. Prove that “If $3n + 2$ is odd for an integer n, then n is odd.”

Proof:

- Assume to the contrary that $3n+2$ is odd, and n is even.
- Since n is even, $n = 2k$, where k is some integer.
- We have $3n + 2 = 6k + 2 = 2(3k + 1)$.
- Thus $3n + 2$ is even, which contradicts the assumption $3n+2$ is odd.
- Therefore, we have proved the theorem “If $3n + 2$ is odd, then n is odd.”

Examples

2. Prove that “If a number added to itself gives itself, then the number is 0.”

Proof:

- Assume to the contrary that $x + x = x$ and $x \neq 0$.
- Then $2x = x$ and $x \neq 0$.
- Because $x \neq 0$, we can divide both sides of the equation by x and arrive at $2 = 1$, which is a contradiction.
- Hence $x + x = x \longrightarrow x = 0$

Exercise

Show that at least three of any 25 days chosen must fall in the same month of the year.

Exercise

Show that at least three of any 25 days chosen must fall in the same month of the year.

Proof:

- Assume to the contrary that any 25 days are chosen and at most 2 days are in the same month of the year.
- Let n_i denote the number of days in the i-th month.
- We have $n_i \leq 2$.
- The total number of chosen days is $n_1 + n_2 + \cdots + n_{12} \leq 24$.
- This contradicts the assumption that 25 days are chosen.
- This completes the proof.

Proof by Cases

- Assume that $P \equiv P_1 \vee P_2 \vee \ldots \vee P_n$.
- Instead of proving $P \longrightarrow Q$, prove

$$(P_1 \longrightarrow Q) \wedge (P_2 \longrightarrow Q) \wedge \ldots \wedge (P_n \longrightarrow Q).$$

- Why?
  - $$\begin{aligned} P_1 \vee P_2 \vee \ldots \vee P_n \longrightarrow Q &\equiv \neg(P_1 \vee P_2 \vee \ldots \vee P_n) \vee Q \\ &\equiv (\neg P_1 \wedge \neg P_2 \wedge \ldots \wedge \neg P_n) \vee Q \\ &\equiv (\neg P_1 \vee Q) \wedge (\neg P_2 \vee Q) \wedge \ldots \wedge (\neg P_n \vee Q) \\ &\equiv (P_1 \longrightarrow Q) \wedge (P_2 \longrightarrow Q) \wedge \ldots \wedge (P_n \longrightarrow Q) \end{aligned}$$

Examples

1. Prove that “If n is an even integer, $4 \le n \le 12$, then n is the sum of two prime numbers.”

Proof:

- We prove this for each value of n:
  - $n = 4 = 2 + 2$
  - $n = 6 = 3 + 3$
  - $n = 8 = 3 + 5$
  - $n = 10 = 5 + 5$
  - $n = 12 = 5 + 7$
- Therefore, this completes the proof.

Credit: Milos Hauskrecht, University of Pittsburgh

Examples

2. Prove that "For any two numbers x and y, $|x||y| = |xy|$."

Proof:

- We prove this by cases. There are 4 cases:
  - Case 1: $x \geq 0, y \geq 0$
    - $xy \geq 0$ and $|xy| = xy = |x||y|$
  - Case 2: $x \geq 0, y < 0$
    - $xy \leq 0$ and $|xy| = -xy = x(-y) = |x||y|$
  - Case 3: $x < 0, y \geq 0$
    - $xy \leq 0$ and $|xy| = -xy = (-x)y = |x||y|$
  - Case 4: $x < 0, y < 0$
    - $xy > 0$ and $|xy| = (-x)(-y) = |x||y|$
- Therefore, $|x||y| = |xy|$.

Credit: Milos Hauskrecht, University of Pittsburgh

Exercise

Prove that “If n is an integer, then $n^2 \geq n$.”

Exercise

Prove that “If n is an integer, then $n^2 \geq n$.”

Proof:

- We consider three cases: $n = 0$, $n \geq 1$, and $n \leq -1$.
- Case 1: $n = 0$
  - $n^2 = 0 = n$.
- Case 2: $n \geq 1$
  - We multiply both sizes of the inequality by n, we obtain $n^2 \geq n$.
- Case 3: $n \leq -1$
  - We have $n^2 \geq 0 \geq n$.
- Because it holds for all cases, we proved the statement.

Disproving a Statement

- Find a counterexample of the statement.
- Example: “Every positive integer is the sum of the squares of two positive integers.”

Proof:

- 3 cannot be written as the sum of the squares of two integers.
- To show this, note that the only possible integers are 0 and 1.
- However, there is no way to write 3 as the sum of two terms each of which is either 0 or 1.

What Makes a Good Proof ?

- State your game plan.
- Keep a linear flow.*
- A proof is an essay, not a calculation.
- Avoid excessive symbolism.
- Revise and simplify.
- Introduce notation thoughtfully.
- Structure long proofs.
- Be wary of the “obvious.”
- Finish.

Proof Strategies

- Understand the definitions.
- Analyze the meaning of the hypothesis and conclusion.
- Prove the statement using one of the proof methods.
- Use forward and backward reasoning.

What is Wrong with the Proof?

1. "The sum of two even numbers is a multiple of 4."

- Proof:
  - Let x and y be even numbers.
  - Then x = 2k and y = 2k, where k is an integer.
  - So x + y = 2k + 2k = 4k, which is a multiple of 4.

x and y may not be equal.

What is Wrong with the Proof?

2. “1/8 > 1/4.”

- Proof:
  - $3 > 2$
  - $\boxed{3 \log_{10}(1/2) > 2 \log_{10}(1/2)}$
  - $\log_{10}(1/2)^3 > \log_{10}(1/2)^2$
  - $(1/2)^3 > (1/2)^2$

The inequality symbol should be reversed when multiplying by a negative number.

What is Wrong with the Proof?

3. “1¢ = $1.”

- Proof:
  - 1¢ = $\boxed{\$0.01 = (\$0.1)^2}$ = (10¢)^2 = $1

$\$ \neq \$^2$