Mathematical Proofs

Cunsheng Ding

HKUST, Hong Kong

September 16, 2015

Contents

Some Inference Rules in Propositional Logic

- Since p is true and $p \to q$, we conclude that q is also true.
  - called, modus ponens.
- Since q is false and $p \to q$, we conclude that p is also false
  - called, modus tollens.
- Since $p \to q$ and $q \to r$, we conclude that $p \to r$.
  - called, hypothetical syllogism.
- Since $p \vee q$ is true and p is false, we conclude that q must be true.
  - called, disjunctive syllogism.

Remark

In predicate logic, we have similar inference rules. In this case, whenever we say that $P(x)$ is true or false, we view x as a specific element in its domain.

Arguments

Definition 1

- An argument in propositional logic is a sequence of propositions.
- All but the final proposition in the argument are called premises, and the final proposition is called the conclusion.
- An argument is valid if the truth of all its premises implies that the conclusion is true.

Example 2

The following is an argument for the conclusion that $5 \leq \sum_{i=1}^{5} i \leq 25$.

Proposition 1: $\sum_{i=1}^{5} i \geq \sum_{i=1}^{5} 1 = 5$ (Premise 1).

Proposition 2: $\sum_{i=1}^{5} i \leq \sum_{i=1}^{5} 5 = 25$ (Premise 2).

Proposition 3: $5 \leq \sum_{i=1}^{5} i \leq 25$ (Conclusion).

Combining Propositions 1 and 2 yields the desired conclusion.

Proofs and Proof Methods

Definition 3

- A proof is a valid and clear argument that demonstrates the truth of a theorem (statement).
- A proof is based on **premises/axioms/definitions** (i.e., statements already assumed/known to be true), and **inference rules**.
- A proof method usually has a form that can be justified by an **inference rule**.

Proving that "$P(x) \Rightarrow Q(x)$" Is True or False

Clarification of terminology

Recall that for any predicate $P(x)$ with domain D, $P(x)$ is either true or false for any specific $x \in D$. So whenever we say $P(x)$ is true or false, we mean the specific proposition $P(x)$ for a specific x in the domain.
By '$P(x) \Rightarrow Q(x)$" being true or false, we mean the same.

Remarks

- Recall $P(x)$ implies $Q(x)$ means "$\forall x \in D, P(x) \rightarrow Q(x)$".
- Recall $P(x)$ implies $Q(x)$ is true if, whenever $P(x)$ is true, $Q(x)$ is also true.
- Recall $P(x)$ implies $Q(x)$ is false if there is any counterexample $x = a$ where $P(a)$ is true and $Q(a)$ is false.

Counter Example Proof for "$P(x) \Rightarrow Q(x)$" Being False

Problem

Prove that "$P(x) \Rightarrow Q(x)$" is false.

How?

Find an element a in the common domain such that $P(a)$ is true and $Q(a)$ is false.

Example 4

Let $P(n)$ be "n is a multiple of 4, and $Q(n)$ be "n is a multiple of 8 with common domain $\mathbb{N}$. Prove that "$P(x) \Rightarrow Q(x)$" is false.

Proof.

Note that $P(4)$ is true, but $Q(4)$ is false. Hence, $n = 4$ is an counterexample. $\square$

Direct Proof for "$P(x) \Rightarrow Q(x)$"

Problem

Prove that "$P(x) \Rightarrow Q(x)$".

How?

Assume $P(x)$ is true. Derive a chain of implications, which ends with $Q(x)$.

Example 5

Prove $x < 0$ implies $x < 1$.

Proof.

Assume that $x < 0$. We want to prove that $x < 1$.

1. By assumption, $x < 0$.
2. We know that $0 < 1$.
3. Combining the two implications above yields $x < 0 < 1$.

□

Proof by Contraposition for "$P(x) \Rightarrow Q(x)$"

Problem

Prove that "$P(x) \Rightarrow Q(x)$" (equivalent to its contrapositive "$\sim Q(x) \Rightarrow \sim P(x)$")

How?

Assume $Q(x)$ is false. Prove that $P(x)$ is also false (it is an indirect proof).

Example 6

Prove $x < 0$ implies $x < 1$.

Proof.

Assume that $x \geq 1$. We want to prove that $x > 0$.

1. By assumption, $x \geq 1$.
2. We know that $1 > 0$.
3. Combining the two implications above yields $x \geq 1 > 0$.

□

Proof by Contradiction for "$P(x) \Rightarrow Q(x)$"

Problem

Prove that "$P(x) \Rightarrow Q(x)$" (it is an indirect proof).

How?

Assume that $P(x)$ is true but $Q(x)$ is false. Then show a contradiction.

Example 7

Prove $xy = 0$ implies $x = 0 \vee y = 0$.

Proof.

Assume that $xy = 0$ and $x \neq 0 \wedge y \neq 0$. We want to derive a contradiction.

1. By assumption, $x \neq 0$ and $y \neq 0$.
2. It then follows that $xy \neq 0$, which is contrary to the assumption that $xy = 0$.

$\square$

Proof of "$\exists x, P(x)$"

How?

Find a value of x such that $P(x)$ is true.

Example 8

Prove that there exists an $x \in \mathbb{N}$ such that $x^2 - 3x + 2 = 0$.

Proof.

We have $x^2 - 3x + 2 = (x - 1)(x - 2)$. Hence $x = 2 \in \mathbb{N}$ is a solution of the equation $x^2 - 3x + 2 = 0$. $\square$

Proof of "$\forall x, P(x)$"

Direct proof

Show that $P(x)$ is true for all values of x in the domain.

Example 9

Prove that $\lfloor (n+1)/2 \rfloor \geq n/2$ for all $n \in \mathbb{N}$.

Proof.

When n is even, $\lfloor (n+1)/2 \rfloor = n/2$.
When n is odd, $\lfloor (n+1)/2 \rfloor = (n+1)/2 > n/2$.
Combining the conclusions in the two cases completes the proof. $\square$

Proof of "$\forall x, P(x)$"

Proof by contradiction

Assume $P(x)$ is false for some value of x in the domain. We want to derive a contradiction.

Example 10

Prove that $x < x^2 + 1$ for all $x \in \mathbb{R}$, the set of real numbers.

Proof.

Assume that $x \geq x^2 + 1$ for some $x \in \mathbb{R}$. We want to derive a contradiction.

- $x \geq x^2 + 1$ and $x^2 + 1 \geq 1$ implies that $x \geq 1$.
- $x \geq x^2 + 1$ and $x^2 + 1 > x^2$ implies that $x > x^2$.
- $x > 1$ and $x > x^2$ implies that $x < 1$.

$x \geq 1$ and $x < 1$ form a contradiction.

$\square$

Indirect Proofs: Two Classical Theorems

Definition 11

Rational numbers are those of the form $\frac{m}{n}$, where $n \in \mathbb{N}$ and $m \in \mathbb{Z}$.

Theorem 12

$\sqrt{2}$ is irrational (not rational).

Proof.

Suppose $\sqrt{2}$ is rational. Then there are two integers m and n such that $\gcd(m, n) = 1$ and $\sqrt{2} = m/n$. We want to derive a contradiction. We have then $m^2 = 2n^2$. It then follows that m is even. Let $m = 2k$ for some integer k. We obtain then

$$n^2 = 2k^2.$$

Hence, n is also even. Consequently, $\gcd(m, n)$ has the factor 2. This is contrary to our assumption that $\gcd(m, n) = 1$. □

Indirect Proofs: Two Classical Theorems

Theorem 13

There are infinitely many prime numbers.

Proof.

Suppose there are only a finite number of primes. Then some prime number p is the largest of all the prime numbers, and hence we can list the prime numbers in ascending order:

$$2, 3, 5, 7, 11, \ldots, p.$$

Let

$$n = (2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times p) + 1.$$

Then $n > 1$, and n cannot be divided by any prime number in the list above. Therefore, n is also a prime. Clearly, n is larger than all the primes in the list. This is contrary to the assumption that all primes are in the list above. $\square$