CS 113: Mathematical Structures for Computer Science

Dr. Francis Parisi

Pace University

Fall 2018

Methods of Proof

Chapter 3

Methods of Proof

- Quantified Statements
- Direct Proof
- Proof by Contrapositive
- Proof by Cases
- Counterexamples
- Existence Proofs
- Proof by Contradiction

Methods of Proof

- It is important to understand proofs of theorems
- This understanding helps us write proofs when needed
- The material in the prior two chapters, Logic and Set Theory, provide the proper background for understanding proofs
- A great way to think of a mathematical proof is as a carefully reasoned argument to convince a that a given statement is true
- If we question or challenge each step and can provide a sound reason we can be sure the proof is correct

Methods of Proof – Quantified Statements

- Open statements involve one or more variables
- An open sentence becomes a statement when a value is assigned to the variable
- Statements can be formed from open sentences by using a quantifier

Methods of Proof – Universal Quantifiers

- Let $R(x)$ be an open sentence over a domain S
- $R(a)$ is a statement for every $a \in S$
- A **universal quantifier** denoted by $\forall$ means "for all," "for every," and "for each."

$$\forall x \in S,\ R(x)$$

is read as

For every $x \in S, R(x)$

Moreover, $\forall x \in S,\ R(x)$ can be expressed as if $x \in S,$ then $R(x)$

Methods of Proof – Existential Quantifiers

- Another way to form a statement from an open sentence by is quantification
- "There exists," "there is" "for some," "for at least one" is each an **existential quantifier**

$$\exists x \in S, Q(x)$$

- There exists $x \in S$ such that $Q(x)$
- For some $x \in S, Q(x)$
- For at least one $x \in S, Q(x)$

Methods of Proof – Negation of Quantified Statements

Definition

For an open sentence $R(x)$ over a domain S, the **negation** of

$$\forall x \in S, R(x)$$

is

$$\sim (\forall x \in S, R(x)) : \text{ It is not the case that } R(x) \text{ for every } x \in S$$

Methods of Proof – Direct Proof

We have seen there are two quantified statements we can construct from the open sentence $R(x)$ with either the universal quantifier

$$\forall x \in S, R(x) \tag{3.1}$$

and the existential quantifier

$$\exists x \in S, R(x) \tag{3.2}$$

Each of (3.1) and (3.2) is a statement thus each has a truth value

Methods of Proof – Direct Proof

- The statement $\forall x \in S, R(x)$ is true if $R(x)$ is true for each $x \in S$. Therefore, $\forall x \in S, R(x)$ is false if $R(x)$ is false for <u>at least</u> one element $x \in S$.
- The statement $\exists x \in S, R(x)$ is true if $R(x)$ is true if there exists at least one element $x \in S$ for which $R(x)$ is true. Consequently, $\exists x \in S, R(x)$ is false if $R(x)$ is false for <u>every</u> element $x \in S$.

Methods of Proof – Direct Proof

- When the domain S contains only a few elements it is easy to show that some statement like (3.1) is true . . . We plug in the values
- But when the domain contains many possibly an infinite number of elements we must provide a *proof*

Definition

A **proof** of a statement is a presentation of a logical argument that demonstrates the truth of the statement

Methods of Proof – Direct Proof

A proof of a statement is typically a sequences of statements following logically and leading to the desired conclusion. We typically make use of:

1. definition of concepts
2. axioms or principles that have been agreed upon
3. assumptions made
4. previous theorems

Methods of Proof – Direct Proof

- To verify that a statement

$$\forall x \in S,\ P(x) \Rightarrow Q(x)$$

is true we use a **direct proof**

- To show that $\forall x \in S,\ P(x) \Rightarrow Q(x)$ is true we must show it is true for all $x \in S$

Remark

To prove that $\forall x \in S,\ P(x) \Rightarrow Q(x)$ is true by means of a direct proof, we assume that $P(x)$ is true for some arbitrary $x \in S$ and then show that $Q(x)$ is true

Methods of Proof – Proof by Contrapositive

The contrapositive of the implication $P \Rightarrow Q$ is $(\sim Q) \Rightarrow (\sim P)$

We also learned that an implication and its contrapositive are equivalent

$$P \Rightarrow Q \;\equiv\; (\sim Q) \Rightarrow (\sim P)$$

We can prove

$$\forall x \in S, P \Rightarrow Q$$

is true if we can show via direct proof that

$$\forall x \in S, (\sim Q) \Rightarrow (\sim P)$$

This is **proof by contrapositive**

Methods of Proof – Proof by Contrapositive

Remark

To prove that $\forall x \in S, P(x) \Rightarrow Q(x)$ is true using a proof by contrapositive, we begin by assuming that $Q(x)$ is false for an arbitrary element of $x \in S$ and then we show that $P(x)$ is also false

Example

Prove: Let n be an integer. If $7n+3$ is an odd integer $[P(x)]$, then n is an even integer $[Q(x)]$.

Proof

Assume n *is not an even integer* $[\sim (Q(x))]$. *Then* n *is an odd integer so* $n = 2k+1$ *for some integer* k. *Therefore,*

$$7n+3 = 7(2k+1)+3 = 14k+10 = 2(7k+5).$$

Since $7k+5$ *is an integer,* $7n+3$ *is even* $[\sim (P(x))]$

Methods of Proof – Proofs of Biconditionals

- Recall that a biconditional $P(x) \Leftrightarrow Q(x)$ is defined as $(P(x) \Rightarrow Q(x)) \wedge (Q(x) \Rightarrow P(x))$
- We want to illustrate how we can prove the quantified statement $\forall x \in S,\ P(x) \Leftrightarrow Q(x)$

Remark

To prove that $\forall x \in S,\ P(x) \Leftrightarrow Q(x)$ is true, we must prove that both $\forall x \in S,\ P(x) \Rightarrow Q(x)$ is true and $\forall x \in S,\ Q(x) \Rightarrow P(x)$ is true

Methods of Proof – Proofs of Biconditionals

- Consider the following theorem...

Theorem

Let n be an integer. Then n^2 is even if and only if n is even.

- This theorem has two conditionals

The “if” part: *If n is even, then n^2 is even*

...and the “only if” part: *If n^2 is even, then n is even*

Methods of Proof – Proofs of Biconditionals

Proof

To prove the implication we start by assuming n is even. Then $n = 2a$ where a is an integer, and

$$n^2 = (2a)^2 = 4a^2 = 2(2a^2).$$

Since $2a^2$ is an integer $2(2a^2)$ is even thus n^2 is even. (Direct Proof)

To prove the converse we assume n is odd. Therefore, $n = 2b + 1$, and b is an integer. We have

$$n^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1.$$

Since $2b^2 + 2b$ is an integer $2(2b^2 + 2b)$ is even so $2(2b^2 + 2b) + 1$ is odd, thus n^2 is odd. (Proof by Contrapositive)

Methods of Proof – Proof by Cases

Example

If n is an integer, then $n^2 - n$ is an even integer.

Let n be an integer and consider the two cases: n is even and n is odd.
Case 1. n is even: Then $n = 2a$ for some integer a and

$$n^2 - n = (2a)^2 - (2a) = 4a^2 - 2a = 2(2a^2 - a)$$

so $n^2 - n$ is even;
Case 2. n is odd: Then $n = 2b + 1$ for some integer b and

$$\begin{aligned} n^2 - n &= (2b+1)^2 - (2b+1) = (4b^2 + 4b + 1) - (2b+1) \\ &= 4b^2 + 2b = 2(2b^2 + b) \end{aligned}$$

so $n^2 - n$ is even.

Methods of Proof – Counterexamples

- Counterexamples allow us to **disprove** statements like $\forall x \in S,\ R(x)$
- To prove $\forall x \in S,\ P(x) \Rightarrow Q(x)$ we must show it is true for all x
- To show $\forall x \in S,\ P(x) \Rightarrow Q(x)$ is false we only need to show it is false for some $a \in S$
- This element $a \in S$ is called a counterexample

Methods of Proof – Existence Proofs

- The proofs we have looked at so far test the truth or falseness of open sentences over an entire domain $\forall x \in S,\ R(x)$
- For quantified statements like $\exists x \in S,\ R(x)$ we need only show that there is *some* element $a \in S$ for which $R(x)$ is true
- This is an **existence proof**.

Example

There exists an integer n such that $2 - n^2 > 0$
Proof: Let $n = 1$ and $2 - n^2 = 2 - 1^2 = 1 > 0$.

Methods of Proof – Proof by Contradiction

- For some mathematical expression $R(x)$ expressed as $\forall x \in S,\ P(x) \Rightarrow Q(x)$ we have used two methods key methods to verify its truth – direct proof and proof by contrapositive
- Another method starts by assuming that R is false, then we deduce a statement that contradicts a known fact or assumption used earlier in the proof
- This is **proof by contradiction**

If P is the fact or assumption from assuming R is false we deduce $\sim P$ we have $\sim R \Rightarrow (P \wedge (\sim P))$. Since $(P \wedge (\sim P))$ is false then $\sim R \Rightarrow (P \wedge (\sim P))$ can only be true if $\sim R$ is false, therefore R is true.

Methods of Proof – Key Results

- For an open sentence $R(x)$ over a domain S

$$\begin{aligned} \sim (\forall x \in S,\ R(x)) &\equiv \exists x \in S,\ \sim R(x) \\ \sim (\exists x \in S,\ R(x)) &\equiv \forall x \in S,\ \sim R(x) \end{aligned}$$

- For an open sentence $R(x, y)$ containing variables x and y, where the domain of x is S and the domain of y is T

$$\begin{aligned} \sim (\forall x \in S,\ \exists y \in T,\ R(x,y)) &\equiv \exists x \in S,\ \forall y \in T,\ \sim R(x,y) \\ \sim (\exists x \in S,\ \forall y \in T,\ R(x,y)) &\equiv \forall x \in S,\ \exists y \in T,\ \sim R(x,y) \end{aligned}$$