Lecture 3

188 200
Discrete Mathematics and Linear Algebra

Pattarawit Polpinit

Department of Computer Engineering
Khon Kaen Uiversity

June 10, 2009

Overview

In the last two lectures, we learned rules of inference which enables us to logically show (prove) that a mathematical statement can be concluded from given premises. This is often called **formal proof**.

In this lecture, we will learn several **informal proof methods**. We will be examining a lot of examples that come from variety of mathematical topics to give you an idea of how to do each proof method.

The best way to learn to proof is to practice. Learning it from watching the slides is like trying to learning tennis from watching TV. So do the exercises!

References

- Chapter 3 : 3.1-3.7

Element of Proof

In mathematics, a proof is

- A sequence of statements that forms an argument.
- Must be correct (well-reasoned, logically valid) and complete (clear, detailed) that rigorously and undeniably establish the truth of a mathematical statement.

In mathematics, we prove

- **Themorem** — a statement that can be shown to be true.
- **Lemma** — a "pre-theorem" or a result that need to be proved to prove the theorem.
- **Corollary** — a "post-theorem" a result which follows directly from the theorem.
- **Conjecture** — a statement believed to be true but for which there is not a good proof yet.
- **Axiom** or **postulates** — statements which are given and assumed to be true.

Formal VS Informal Proof

Using rules of inference, we can construct a formal proof that is precise and complete.

- "easy" for machine to construct.

However, we cannot always use formal proof techniques.

- Formal proof are usually tedious for human to construct.

Most mathematical proofs are actually constructed using **informal proof** techniques.

Characteristics of an Informal Proof

In an informal proof

- The statements making up the proof are typically not written in any formal language (e.g., propositional logic)
- Steps of the proof and derivations are often argued using English or mathematical formulas
- Multiple derivations may occur in a single step
- Axioms are often not all stated up front

As a result, it is sometimes easy to make mistakes writing informal proofs.

Methods of Proof

In this lecture, we will be discussing the following methods of proof:

- Direct Proofs
- Proof by Contraposition (Indirect Proofs)
- Proof by Contradiction
- Vacuous Proofs
- Trivial Proofs
- Proof by Cases
- Proof of Equivalences
- Existence Proofs
- Uniqueness Proofs
- Counterexamples

Direct Proof

Proof of a statement : $P \rightarrow Q$

Assume P is true and show that Q must therefore be true.

Example If n is odd integer, n^2 is odd.

Definition An integer n is even iff $n = 2k$ for some integer k. n is odd iff $n = 2k + 1$ for some integer k.

Let $P(x)$ denote x is an odd integer

$Q(x)$ denote x^2 is odd integer.

$P(n) \rightarrow Q(n)$

Direct Proof : Example 1 continues

Proof:

- We first assume $P(n)$ is true, i.e. n is odd.
- We want to show $Q(n)$ is true, i.e. n^2 is odd.
- By definition, $n = 2k + 1$ where k is some integer.
- Therefore

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

which is by the definition is an odd number ($k' = 2k^2 + 2k$)

Q.E.D.

Direct Proof : Example 2

Example: Prove the following statement using direct proof: If the sum of any two integers is even, then their difference is even.

- For any two integer x and y, if $x + y$ is even, $x - y$ is even.

Proof

-
-
-
-

Q.E.D.

Proof by Contrapositive

Sometimes it is difficult to do a direct proof, we can try proving its contrapositive.

- The contrapositive of $P \rightarrow Q$ is $\neg Q \rightarrow \neg P$ which is logically equivalent to $P \rightarrow Q$.
- Thus show that if $\neg Q$ is true then $\neg P$ is true.

Example Show that if a and b are integers, and $a + b \geq 15$ then $a \geq 8$ or $b \geq 8$.

Let P be "$a + b \geq 15$" and Q be "$a \geq 8$ or $b \geq 8$".

Proof :

1. (Assume $\neg Q$) Suppose that $a < 8$ and $b < 8$.
2. We want to show $\neg P$, i.e. $a + b < 15$.
3. From 1, $a \leq 7$ and $b \leq 7$ (a and b are integers).
4. implies $a + b \leq 14$.
5. implies $a + b < 15$.
6. $\neg Q \rightarrow \neg P$ is true, therefore $P \rightarrow Q$ must be true. Q.E.D.

Try proving it with direct proof. See if it's easier.

Example 2: Proof by Contrapositive

Theorem For integer n, if $3n + 2$ is odd then n is odd.

$(3n + 2$ is odd$) \rightarrow (n$ is odd$)$.

Proof

-
-
-
-
-

Q.E.D.

Again try proving it with direct proof, see which one is easier.

When do you use direct proof or indirect proof?

– If it is not clear from the problem, try direct first.

Proof by Contradiction

We want to prove P.

1. Assume $\neg P$ is true, and then prove $\neg P \rightarrow \mathbf{F}$ must be true (i.e. a false statement or contradiction such as $R \wedge \neg R$).
2. We conclude that $\neg P$ is false since 1. is true and therefore P is true. ($\neg P \rightarrow \mathbf{F}$ is true iff $\neg P$ is true.)

We want to prove $P \rightarrow Q$.

1. Assume the negation of the conclusion is true, i.e., $\neg Q$.
2. Prove that $(P \wedge \neg Q) \rightarrow \mathbf{F}$ is true.
3. Since 2. is true, $P \wedge \neg Q$ must be false.
   - implies $P \rightarrow Q$ is true.
   - Because $\neg(P \rightarrow Q) \equiv \neg(\neg P \vee Q) \equiv P \wedge \neg Q$

Example : Proof by Contradiction

Prove the following Example by formal proof using contradiction proof technique.

Example: Consider the following statements

- Rainy day makes gardens grow. $\longleftarrow$ $R \rightarrow G$
- Gardens don't grow if it is not hot. $\longleftarrow$ $\neg H \rightarrow \neg G$
- When it cold outside, it rains. $\longleftarrow$ $\neg H \rightarrow R$

Prove that it is hot. $\longleftarrow$ H

Let

- R—rainy day
- G — gardens grow
- H — it is hot.

Note: We will assume that "cold" is equivalent to "not hot".

Example : Proof by Contradiction II

Proof :

Step	**Reason**
1. $R \rightarrow G$	Given
2. $\neg H \rightarrow \neg G$	Given
3. $\neg H \rightarrow R$	Given
4. $\neg H$	Assume false by contradiction proof
5. R	Modus ponens from 3 and 4
6. G	Modus ponens from 1 and 5
7. $\neg G$	Modus ponens from 2 and 4
8. $G \wedge \neg G$	Contradiction.

Because Premises $\wedge \neg H \rightarrow$ **F** is true

Premises $\rightarrow H$ must be true.

$\therefore H$ Q.E.D.

Example : Proof by Contradiction

Theorem If a^2 is even then a is even.

Proof: Proof by contradiction.

Let P denote a^2 is even, and Q denote a is even.

Given that P is true, we assume $\neg Q$ is true. Find a contradiction.

$\neg Q$: a is odd, namely $a = (2k + 1)$ for some integer k.

Then $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

This implies that a^2 is odd. $\longleftarrow$ **Contradiction!**

Since $P \wedge \neg Q \rightarrow \mathbf{F}$, then we can conclude that $P \rightarrow Q$ must be true.

$\therefore$ a is even. Q.E.D.

Example 2 : Proof by Contradiction

Let's revisit a preciously proved Theorem.

Theorem For integer n, if $3n + 2$ is odd then n is odd.

$(3n + 2$ is odd$) \rightarrow (n$ is odd$)$.

Proof:

-
-
-
-
-

Q.E.D.

Example 3 : Proof by Contradiction

Theorem Show that $\sqrt{2}$ is irrational.

Definition A real number r is rational iff $r = a/b$ for some integer a and b with $b \neq 0$. Real number that is not rational is irrational.

Proof: We will prove by contradiction. Suppose $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = a/b$ for some integer a and b such that a and b have **no factor in common** (e.g. a:1 b:2, a:3 b:7).

$$\sqrt{2} = a/b \ \rightarrow \ 2 = a^2/b^2 \ \rightarrow \ 2b^2 = a^2$$

This implies that a^2 is even, so a is even (from the previous theorem). So by definition of even number $a = 2k$ for some integer k. So

$$2b^2 = a^2 \ \rightarrow \ 2b^2 = (2k)^2 \ \rightarrow \ 2b^2 = 4k^2 \ \rightarrow \ b^2 = 2k^2$$

This implies that b^2 is even, so b is even. **But if both a and b are even, they have a common factor**. **Contradiction!**

$\therefore \sqrt{2}$ is irrational. Q.E.D.

Example 4 : Proof by Contradiction

Theorem There are infinitely prime numbers.

Definition An integer n is prime iff $n > 1$ and for all positive integers r and s, if $n = r \cdot s$, then $r = 1$ or $s = 1$. The opposite of prime number is composite number.

Proof : We will prove by contradiction. Let P denote "There are infinitely many prime number".

Assume $\neg P$, i.e., there a finite number of prime numbers. Let call the largest prime number n_r.

Let define R the product of all prime numbers, i.e.,
$R = n_1 x n_2 \ldots n_r$.

Example 4 : Proof by Contradiction II

Now consider $R + 1$. $R + 1$ is either prime or not prime (a number is either prime or composite.)

- If it's prime we have a prime number larger than n_r. $\longleftarrow$ **Contradiction !**
- If it's not prime, let n^* be a prime number dividing $R + 1$. But n^* cannot be any of $n_1 x n_2 \ldots n_r$. So n^* must be larger than n_r. $\longleftarrow$ **Again Contradiction !**

These contradicts our assumption that there is a finite number of primes, therefore such statement must be false. This mean there must be infinite number of primes.

Q.E.D.

Vacuous Proofs

- Consider an implication $P \longrightarrow Q$.
- If it can be shown that P is false, then the implication is always true.
- So we show that P is false.

Example Consider the following statements:

- All students with laws major in 188 200 are male.
- In other words, if you are majoring in laws and you are taking 188 200, then you are male.

Since there are no laws major in this class, then the antecedent is false and the implication is true.

Q.E.D.

Trivial Proofs

- Again consider an implication $P \rightarrow Q$
- If it can be shown that Q is true, then the implication is always true.
- So we show that the conclusion is always true.

Example Consider the statement "If you are smart and are in 188 200, then you like computers.

Since everyone in this room like computers, the statement is always true regardless of how smart you are.

Q.E.D.

Proof by Cases

To prove a statement which can be divided into several smaller cases, we show that all cases are true. Thus we are showing a statement of the form

$$(P_1 \vee P_2 \vee \ldots \vee P_n) \rightarrow Q.$$

We use the tautology

$$((P_1 \vee P_2 \vee \ldots \vee P_n) \rightarrow Q) \leftrightarrow (P_1 \rightarrow Q) \wedge (P_2 \rightarrow Q) \wedge \ldots \wedge (P_n \rightarrow Q)$$

Example : Show that for any integer n,

$$\lfloor n/2 \rfloor = \begin{cases} n/2 & \text{if } n \text{ is even} \\ (n-1)/2 & \text{if } n \text{ is odd} \end{cases}$$

Definition : Given a real number x, the floor of x, denoted $\lfloor x \rfloor$, is equal to an integer n where n is the largest number such that $n \leq x$. The ceiling of x, denoted $\lceil x \rceil$, is equal to an integer n where n is the smallest number such that $n \geq x$.

Example : Proof by Cases

Proof : Suppose n is an integer n must be either odd or even.

Case 1 (n is odd) : In this case $n = 2k + 1$ for some integer k.
By substitution,
$\lfloor n/2 \rfloor = \lfloor (2k + 1)/2 \rfloor = \lfloor k + 1/2 \rfloor = k$
because k is largest integer such that $k \leq k + 1/2$.
But since $n = 2k + 1$, so $k = (n - 1)/2$.
$\therefore \lfloor n/2 \rfloor = (n - 1)/2$.

Case 2 (n is even) : In this case $n = 2k$ for some integer k. By substitution, $\lfloor n/2 \rfloor = \lfloor (2k)/2 \rfloor = k$.
But since $n = 2k$, so $k = n/2$. $\therefore \lfloor n/2 \rfloor = n/2$.

The combination of both cases proves the result.

Q.E.D.

Note: Make sure you get all the cases. The biggest mistake is to leave out some of the cases.

Proof of Equivalences

Recall that $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$.

So to prove $P \leftrightarrow Q$, we must show $P \rightarrow Q$ and $Q \rightarrow P$ which can be done by any other proof methods.

The validity of this proof result comes from the fact that

$(P \leftrightarrow Q) \leftrightarrow ((P \rightarrow Q) \wedge (Q \rightarrow P))$ is tautology.

Example Prove that n is odd iff n^2 is odd.

Proof : There are two parts to be shown:

1. If n is odd than n^2 is odd.
2. If n^2 is odd then n is odd.

Both must be true to make the statement true.
(1) is proved in Example 2 : Direct Proof. Prove (2) using method of your choice.

Q.E.D.

Existential Proofs

Given a statement : $\exists x\ P(x)$, how do we show it is true?

We only have to show that $P(c)$ is true for some value of c.

There are two types of existential proofs:

1. **Constructive proofs** — find a specific value of c for which $P(c)$ exists.
2. **Non-constructive proofs** — show that such a c exists, but do not actually find it.
   — Assume that it does not exist, and show a contradiction.

Example : Existential Proofs

Constructive existence proof examples

Show that a square exists that is the sum of two other squares

Proof : $3^2 + 4^2 = 5^2$. Q.E.D.

Show that a cube exists that is the sum of three other cubes.

Proof : $3^3 + 4^3 + 5^3 = 6^3$ Q.E.D.

Example 2 : Existential Proofs

Non-constructive existence proof examples

Prove that either $2 \cdot 10^{500} + 15$ or $2 \cdot 10^{500} + 16$ is not a perfect square.

- A perfect square is a square of an integer.
- In other words: show that a non-perfect square exists in the set $\{2 \cdot 10^5 00 + 15$ or $2 \cdot 10^5 00 + 16\}$.

Proof : The only two perfect squares that differ by 1 is 0 and 1.

- Thus, any other numbers that differ by 1 cannot both be perfect squares
- Thus, a non-perfect square must exist in any set that contains two numbers that differ by 1

Q.E.D.

Note that we didn't specify which one it was!

Uniqueness Proofs

A theorem may state that only one such value exists.

To prove this, you need to show

- **Existence** : that such a value does indeed exist.
  – Either via a constructive or non-constructive existence proof.
- **Uniqueness** : that there is only one such value.

Example If the real number equation $5x + 3 = a$ has a solution, then it is unique.

Proof : Show existence

- We can manipulate the equation to get $x = (a - 3)/5$

Is this constructive or non-constructive?

Uniqueness Proofs II

Proof (Continue.)

Show uniqueness:

- If there are two such number, say x and y, they would fulfill the following $a = 5x + 3 = 5y + 3$.
- We can manipulate this to get $x = y$. Thus the one solution is unique.

Counterexample

Given a universal quantified statement, find a single example that is not true.

This is to disprove a statement, i.e., to show that a statement is false.

Example : Every months have 31 days.'

Proof : May has 30 days. Q.E.D.

Example :Every positive integer is the square of another integer.

Proof: The square root of 5 is approximately 2.23 which is not an integer. Q.E.D.

Counterexamples II

You can disprove a universal statement by showing a single counterexample.

You cannot prove a universal statement by example.

Example : prove or disprove that all numbers are even.

- Counterexample: 1 is not even.
- Proof by example: 2 is even $\longleftarrow$ invalid.

Common Mistakes in Proofs

Affirming the conclusion:

$P \rightarrow Q$ is true, and Q is true, so P must be true.

No because, as we know it, $\mathbf{F} \rightarrow \mathbf{T}$ is true.

Example : Consider the following statements:

- You will get a grade
- If you are in this class, you will get a grade.

Let p denote "You are in this class"
q denote "You will get a grade"

$$\begin{array}{l} Q \\ P \rightarrow Q \\ \therefore P \end{array}$$

You cannot conclude that you are in this class

– You could be getting a grade from another class. 2

Common Mistakes in Proofs II

Denying the hypotheses

$P \to Q$ is true, and P is false, so Q must be false.

No again because $\mathbf{F} \to \mathbf{T}$ and $\mathbf{F} \to \mathbf{F}$ are true.

Example : Consider the following statements:

- you are not in this class
- if you are in this class you will get a grade.

$\neg P$

$P \to Q$

$\therefore \neg Q$

You cannot conclude that you will not get a grade.

– You could be getting a grade for another class.