01204211 Discrete Mathematics
Lecture 4: Proof techniques 1

Jittat Fakcharoenphol

September 21, 2015

Proof techniques[1]

Using inference rules, we can prove facts in propositional logic. However, in many cases, we want to prove wider range of mathematical facts. Inference rules play crucial parts in providing high-level structures for our proofs.

[1] This lecture mostly follows Berkeley CS70 lecture notes.

Proof techniques[1]

Using inference rules, we can prove facts in propositional logic. However, in many cases, we want to prove wider range of mathematical facts. Inference rules play crucial parts in providing high-level structures for our proofs.
In this lecture, we will focus on two general proof techniques that originate from two simple inference rules.

- Direct proofs
- Proofs by contraposition

[1] This lecture mostly follows Berkeley CS70 lecture notes.

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)
- To prove a theorem, we may prove many simple lemmas to make our argument. A **lemma**, in this sense, is a smaller theorem (or a supportive one).

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)
- To prove a theorem, we may prove many simple lemmas to make our argument. A **lemma**, in this sense, is a smaller theorem (or a supportive one).
- A **corollary** is a theorem which is a "fairly" direct result of other theorems.

Terminologies

These are terminologies used when showing mathematical facts.

- A **theorem** is a statement that can be argued to be true.
- A **proof** is the sequence of statements forming that mathematical argument.
- An **axiom** is a statement that is assumed to be true. (Note that we do not prove an axiom; therefore, the validity of a theorem proved using an axiom relies of the validity of the axiom.)
- To prove a theorem, we may prove many simple lemmas to make our argument. A **lemma**, in this sense, is a smaller theorem (or a supportive one).
- A **corollary** is a theorem which is a "fairly" direct result of other theorems.
- A **conjecture** is a statement which we do not know if it is true or false.

Fermat's Last Theorem

Theorem: No three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ when $n > 2$.

This theorem has been conjectured by Pierre de Fermat in 1637. It remained a conjecture until Andrew Wiles proved it in 1994.

Goldbach's conjecture

Conjecture: Every even integer greater than 2 can be expressed as the sum of two primes.

In 1742, Christian Goldbach proposed this cojecture to Leonhard Euler. It remains unsolved.

Euclid's axioms

Euclidean geometry is defined by the following 5 postulates (axioms).

1. A straight line segment can be drawn joining any two points.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having the segment as radius and one endpoint as center.
4. All right angles are congruent.
5. (The parallel postulate) If two lines are drawn which intersect a third in such a way that the sum of the inner angles on one side is less than two right angles, then the two lines inevitably must intersect each other on that side if extended far enough.

References: Weisstein, Eric W. "Euclid's Postulates." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/EuclidsPostulates.html

The triangle postulate

The following statement is called the triangle postulate.

The sum of the angles in every triangle is 180^o.

The only way to prove this in Euclidean geometry is to use the parallel postulate. (Exercise: try to prove it.)

The triangle postulate

The following statement is called the triangle postulate.

> The sum of the angles in every triangle is 180^o.

The only way to prove this in Euclidean geometry is to use the parallel postulate. (Exercise: try to prove it.)
Is this statement always true everywhere in the world (or in the universe)?

The triangle postulate

The following statement is called the triangle postulate.

> The sum of the angles in every triangle is 180^o.

The only way to prove this in Euclidean geometry is to use the parallel postulate. (Exercise: try to prove it.)
Is this statement always true everywhere in the world (or in the universe)?
There are other geometries where Euclid's 5^{th} postulate is not true; then the triagle postulate may not be true in those cases. Can you imagine one?

Direct proofs

When we want to prove a theorem of the form $P \Rightarrow Q$, we can assume that P is true, then use this to argue that Q has to be true as well.

Direct proofs

Theorem:
$P \Rightarrow Q$.

Proof.
Assume P.
... (then show that Q follows from P) $\square$

Example 1

Theorem 1

If x is an even number, then x^2 is an even number.

Example 1

Theorem 1

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.

Example 1

Theorem 1

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.

By definition, there exists an integer k such that $x = 2k$.

Example 1

Theorem 1

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.
By definition, there exists an integer k such that $x = 2k$. This implies that $x^2 = (2k)^2 = 4k^2$.

Example 1

Theorem 1

If x is an even number, then x^2 is an even number.

Proof.

Assume that x is an even number.

By definition, there exists an integer k such that $x = 2k$. This implies that $x^2 = (2k)^2 = 4k^2$. Since k is an integer, $2k^2$ is also an integer. Hence we can write $x^2 = 2 \cdot (2k^2)$ where $2k^2$ is an integer; this means that x^2 is even. $\square$

Example 1: disected

Theorem 2

($\forall x$) If x is an even number, then x^2 is an even number.

Example 1: disected

Theorem 2

($\forall x$) If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$ where $P(x) =$ "x is an even number".

Example 1: disected

Theorem 2
($\forall x$) If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$ where $P(x) =$ "x is an even number".
- By definition, $P(x) \Rightarrow R(x)$ where $R(x) =$"there exists an integer k such that $x = 2k$."

Example 1: disected

Theorem 2

($\forall x$) If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$ where $P(x) =$ "x is an even number".
- By definition, $P(x) \Rightarrow R(x)$ where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \Rightarrow S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."

Example 1: disected

Theorem 2

($\forall x$) If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$ where $P(x) =$ "x is an even number".
- By definition, $P(x) \Rightarrow R(x)$ where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \Rightarrow S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."
- By elementary algebra, we know that U is true, where $U =$ "for all integer k, $2k^2$ is an integer."

Example 1: disected

Theorem 2

$(\forall x)$ If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$ where $P(x) =$ "x is an even number".
- By definition, $P(x) \Rightarrow R(x)$ where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \Rightarrow S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."
- By elementary algebra, we know that U is true, where $U =$ "for all integer k, $2k^2$ is an integer."
- $S(x) \wedge U \Rightarrow V(x)$, where $V =$ "there exists an integer k such that $x^2 = 2 \cdot (2k^2)$ where $2k^2$ is an integer."

Example 1: disected

Theorem 2

$(\forall x)$ If x is an even number, then x^2 is an even number.

Proof.

- Assume $P(x)$ where $P(x) =$ "x is an even number".
- By definition, $P(x) \Rightarrow R(x)$ where $R(x) =$"there exists an integer k such that $x = 2k$."
- $R(x) \Rightarrow S(x)$, where $S(x) =$ "there exists an integer k such that $x^2 = (2k)^2 = 4k^2$."
- By elementary algebra, we know that U is true, where $U =$ "for all integer k, $2k^2$ is an integer."
- $S(x) \wedge U \Rightarrow V(x)$, where $V =$ "there exists an integer k such that $x^2 = 2 \cdot (2k^2)$ where $2k^2$ is an integer."
- By definition, $V(x) \Rightarrow Q(x)$, where $Q(x) =$ "x^2 is even".

$\square$

Example 1: be careful

When we prove a statement with universal quantifiers like:

$(\forall x)$ If x is an even number, then x^2 is an even number

we have to be *extremely* careful not to assume anything about x except those state explicitly in the assumption.

Practice: Back to our subgoal

Can you use direct proofs to show the following theorem?

Theorem 3

For any positive number n and a such that $a > \sqrt{n}$, then $n/a \leq \sqrt{n}$.

Practice: Back to our subgoal

Can you use direct proofs to show the following theorem?

Theorem 3

For any positive number n and a such that $a > \sqrt{n}$, then $n/a \leq \sqrt{n}$.

Proof.

Assume that $a > \sqrt{n}$.

Practice: Back to our subgoal

Can you use direct proofs to show the following theorem?

Theorem 3

For any positive number n and a such that $a > \sqrt{n}$, then $n/a \leq \sqrt{n}$.

Proof.

Assume that $a > \sqrt{n}$. Since

$$n = n,$$

by dividing the left side by a and the right side by $\sqrt{n}$, we get that

$$\frac{n}{a} < \frac{n}{\sqrt{n}},$$

because both a and $\sqrt{n}$ are positive. Hence, $n/a < \sqrt{n}$ as required. □

Practice: Divisibility by 3 (1)

Let's try to prove a well-known fact.

Theorem 4

An integer n is divisible by 3 if the sum of the digits of n is divisible by 3.

Practice: Divisibility by 3 (1)

Let's try to prove a well-known fact.

Theorem 4

An integer n is divisible by 3 if the sum of the digits of n is divisible by 3.

Let's start by proving this lemma.

Lemma 5

For any integer $k \geq 0$, $10^k - 1$ is divisible by 3.

Practice: Divisibility by 3 (2)

Proof.

Assume that the sum of the digits of n is divisible by 3. We will show that n is divisible by 3.

Let k be the number of digits of n. Let $a_1, a_2, \ldots, a_k$ be the digits of n where a_1 is the most significant digit and a_k is the least significant one. Therefore, we can write

$$n = a_1 \cdot 10^{k-1} + a_2 \cdot 10^{k-2} + \cdots + a_{k-1} \cdot 10^1 + a_k \cdot 10^0.$$

Consider the i-th term: $a_i \cdot 10^{k-i-1}$. From Lemma 5, we know that $10^{k-i-1} - 1$ is divisible by 3. Thus $a_i \cdot (10^{k-i-1} - 1)$ is also divisible by 3. Therefore, the remainder of $a_i \cdot 10^{k-i-1}$ divided by 3 is equal to the remainder of a_i divided by 3.

Summing all terms, the remainder of the division of n by 3 is $a_1 + a_2 + \cdots + a_k$. Since 3 divides this number, the remainder of $n/3$ is 0; thus, 3 divides n. $\square$

Proof by contraposition

When we want to prove a theorem of the form $P \Rightarrow Q$, we can assume that Q is false, then use this to argue that P has to be false as well.

Proof by contraposition

Theorem:
$P \Rightarrow Q$.

Proof.
Assume $\neg Q$.
... (then show that $\neg P$ follows from $\neg Q$) $\square$

Practice

Theorem 6

If x^2 is an even number, then x is an even number,

Practice

Theorem 6

If x^2 is an even number, then x is an even number,

Before we try to prove by contraposition, let's try to use direct proof to show this theorem.

Practice

Theorem 6

If x^2 is an even number, then x is an even number,

Before we try to prove by contraposition, let's try to use direct proof to show this theorem.

Proof.

Assume that x^2 is an even number...

Practice

Theorem 6

If x^2 is an even number, then x is an even number,

Before we try to prove by contraposition, let's try to use direct proof to show this theorem.

Proof.

Assume that x^2 is an even number...

... doesn't seem to go very well. $\square$

Practice

Theorem 7

If x^2 is an even number, then x is an even number,

Practice

Theorem 7

If x^2 is an even number, then x is an even number,

Proof.

We will prove by contraposition. Assume that x is not an even number.

$\square$

Proving iff statements

How can we prove a statement of the form $P \Leftrightarrow Q$? For example:

Theorem 8

x is an even number iff x^2 is an even number.

Proving iff statements

How can we prove a statement of the form $P \Leftrightarrow Q$? For example:

Theorem 8

x is an even number iff x^2 is an even number.

Proof.

We will prove that the statement is true in both directions.
($\Rightarrow$) This direction is true from Theorem 1.
($\Leftarrow$) This direction is true from Theorem 5. $\square$

An incorrect proof is not a proof

Theorem 9

For any numbers x and y, $x = y$.

An incorrect proof is not a proof

Theorem 9

For any numbers x and y, $x = y$.

Proof.

Assume that

$$x = y.$$

An incorrect proof is not a proof

Theorem 9

For any numbers x and y, $x = y$.

Proof.

Assume that

$$x = y.$$

Multiplying both terms by 0, we get that

$$0 \cdot x = 0 \cdot y,$$

An incorrect proof is not a proof

Theorem 9

For any numbers x and y, $x = y$.

Proof.

Assume that

$$x = y.$$

Multiplying both terms by 0, we get that

$$0 \cdot x = 0 \cdot y,$$

and this implies

$$0 = 0,$$

which is clearly true. $\square$

An incorrect proof is not a proof

Theorem 9

For any numbers x and y, $x = y$.

Proof.

Assume that

$$x = y.$$

Multiplying both terms by 0, we get that

$$0 \cdot x = 0 \cdot y,$$

and this implies

$$0 = 0,$$

which is clearly true. $\square$

What is wrong with this (non) proof?

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.
But you can get better by (1) trying to read and understand good proofs and by (2) practicing.

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.
But you can get better by (1) trying to read and understand good proofs and by (2) practicing.

There are many levels of understandings:

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.
But you can get better by (1) trying to read and understand good proofs and by (2) practicing.

There are many levels of understandings:

- Understand each step of the proof and how each step follows from previous ones

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.
But you can get better by (1) trying to read and understand good proofs and by (2) practicing.

There are many levels of understandings:

- Understand each step of the proof and how each step follows from previous ones
- Understand why the proof needs each step

How to be good at proving theorems?

In a way, proving theorems is like solving puzzles. There is no general rules on how to prove theorems.
But you can get better by (1) trying to read and understand good proofs and by (2) practicing.

There are many levels of understandings:

- Understand each step of the proof and how each step follows from previous ones
- Understand why the proof needs each step
- Can apply techniques or proof strategies learned from this proof for proving other statements