01204211 Discrete Mathematics Lecture 3a: Proof techniques 1

Jittat Fakcharoenphol

July 10, 2021

Proof techniques¹

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.

¹This lecture mostly follows Berkeley CS70 lecture notes. → ⟨ ≥ ⟩

Proof techniques¹

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 $P \Rightarrow Q$, Assume P, Interpretable QProofs by contraposition

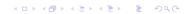
7Q -> 7P Assuma 7Q, Inium wa Trun 7P

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
 - A proof is the sequence of <u>statements</u> 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.



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.	
\dots (then show that Q follows from P)	

Theorem 1

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

$$(\forall x)$$
, $P(x) \rightarrow Q(x)$

Theorem 1

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

Proof.

Assume that x is an even number.

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.

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 $x^2=(2k)^2=4k^2$.

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.

Theorem 2

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

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".

Theorem 2

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

- 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."

Theorem 2

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

- 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 $x^2 = (2k)^2 = 4k^2$."

Theorem 2

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

- 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."

Theorem 2

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

- 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."
- $S(x) \land U \Rightarrow V(x)$, where V = "there exists an integer k such that $x^2 = 2 \cdot (2k^2)$ where $2k^2$ is an integer."

Theorem 2

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

- 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".

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 <u>extremely</u> 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

$$\left(\frac{n}{a} < \frac{n}{\sqrt{n}},\right) = \sqrt{n}$$

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

Practice: Divisibility by 3 (1)
$$3 | 3 | 3 | 9$$
 $3 | 12 | 1+2=3$ $3 | 123 | 1+2+3=6$ Let's try to prove a well-known fact. $3 | 1122 | 14+2+2=6$

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 $k \ge 0$, $10^k - 1$ is divisible by 3.

$$3 \ln n^{3/3}$$
 | $9 \times 10^{k-1} + 9 \times 10^{k-2} + \cdots + 9 \times 10^{k-1}$ | เนื่องอาก 3 บน 9 คงคำ จึงบน ทุ า พานใน ผลราง องคำกัง พ

Practice: Divisibility by 3 (2)



Proof.

Assume that the <u>sum of the digits of n is divisible by 3.</u> We will show that n is divisible by 3.

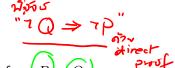
Let k be the number of digits of n. Let a_1, a_2, \ldots, a_k be the digits of n where a_1 is the most significant digit and a_k is the least significant one. Therefore, we can write

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

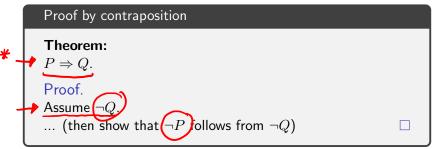
Consider the i-th term: $a_i \cdot 10^{k-i}$. From Lemma 5, we know that $10^{k-i}-1$ is divisible by 3. Thus $a_i \cdot (10^{k-i}-1)$ is also divisible by 3. Therefore, the remainder of $a_i \cdot 10^{k-i}$ divided by 3 is equal to the remainder of a_i divided by 3.

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.

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.



Practice converted (If x is an even number)

Theorem 6

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

If x^2 is an even number, then \underline{x} is an even number,

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.

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...

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.



Theorem 7

= x Juou. of

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

2 15494. 8

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. นีน ถืง χ เป็น จิง เป็น จิง หัวนาเก็ม k หั

$$x=2k+1.$$

$$|\hat{k}_{4}| \propto^{2} (2k+1)^{2} = (2k)^{2} + 2 \cdot 2k \cdot 1 + 1^{2}$$

= $4k^{2} + 4k + 1 = 2 \cdot (2k^{2} + 2k) + 1$

100 γ 10 γ

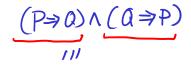
Proving iff statements

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.

- \checkmark (\Rightarrow) This direction is true from Theorem 1.
- \checkmark (\Leftarrow) This direction is true from Theorem 5. \checkmark

Theorem 9 For any numbers x and y, x = y.

Theorem 9

For any numbers x and y, x = y.

Proof.

Assume that

$$x = y$$
.

Theorem 9

For any numbers x and y, x = y.

Proof.

Assume that

$$x = y$$
.

Multiplying both terms by 0, we get that

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

Thm: P

Theorem 9

For any numbers x and y, x = y.

Proof.

Assume that



Multiplying both terms by 0, we get that

$$\underbrace{0 \cdot x} = \underbrace{0 \cdot y},$$

and this implies

which is clearly true.

Assum P





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.

What is wrong with this (non) proof?

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

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:

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

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

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

my

Understand why the proof needs each step

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
- Understand each step of the proof and how each step follows from previous ones
- Why
- ▶ Understand why the proof needs each step
- use
- ► Can apply <u>techniques or proof strategies</u> learned from this proof for proving other statements