01204211 Discrete Mathematics
Lecture 3b: Proof techniques 2

Jittat Fakcharoenphol

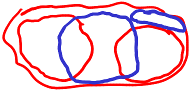
July 10, 2021

Proof techniques[1]

In this lecture, we will focus on two other proof techniques.

- Proofs by contradiction *
- Proofs by cases $\leftarrow$

(exhaustion)



$P \leftarrow$ สมมติให้ P เป็นเท็จ

สมมติ $\neg P$

$\downarrow$

$F \cdots R \land \neg R$

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

Proofs by contradiction

We want to prove that proposition P is true. To do so, we first assume that P is false, and show that this logically leads to a contradiction. This means that it is impossible for P to be false; hence, P has to be true. This is called a proof by contradiction or *reductio ad absurdum*.

Direct proofs

Theorem:
P

Proof.
We use prove by contradiction.
Assume $\neg P$.
... (then show that R and $\neg R$ follows from $\neg P$)
This is a contradiction. Therefore, P must be true. □

Example 1 (1)

rational number
(จน.ตรรกยะ) คือจำนวนที่
สามารถเขียนให้อยู่ในรูปของ
เศษส่วน a/b โดยที่
a และ b เป็น จน.เต็ม

Theorem 1
$\sqrt{2}$ *is irrational.*

$$\left[\forall a,b \in \mathbb{Z},\ \frac{a}{b} \neq \sqrt{2}\right]$$

Proof.
We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.

Example 1 (1)

⌜ x เป็น จน.คู่ $\Longleftrightarrow x^2$ เป็น จน.คู่ ⌟

Theorem 1

$\sqrt{2}$ is irrational.

Proof.

We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.
Therefore, there exists a pair of positive integers a and b such that $\sqrt{2} = a/b$.

Example 1 (1)

$\frac{4}{2}$ $\frac{3}{4}$ $\frac{100}{50}$

Theorem 1

$\sqrt{2}$ is irrational.

Proof.

We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.

Therefore, there exists a pair of positive integers a and b such that $\sqrt{2} = a/b$. Let's choose the pair a and b such that b is minimum. In this case, a and b share no common factors.

Example 1 (1)

Theorem 1

$\sqrt{2}$ is irrational.

Proof.

P

We prove by contradiction. Assume that the theorem is false, i.e., assume that $\sqrt{2}$ is rational.

Therefore, there exists a pair of positive integers a and b such that

$\neg P$

$\sqrt{2} = a/b$. Let's choose the pair a and b such that b is minimum. In this case, a and b share no common factors.

Let's square both terms. We get $2 = a^2/b^2$, or

$$a^2 = 2b^2.$$

(cont. in next slide) □

Example 1 (2)

b จนเต็ม

b^2 จน.เต็ม

$a^2 = 2b^2 \Rightarrow a^2$ คู่

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number.

Example 1 (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number. Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$.

Example 1 (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number. Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$. This implies that b^2 is an even number. Again, this means that b must be an even number.

◀ PAUSE ▶ $\sqrt{2} = \frac{a}{b}$ โดยที่ a, b ไม่มีตัวประกอบร่วม

Example 1 (2)

Proof. (cont.)

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number. Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$. This implies that b^2 is an even number. Again, this means that b must be an even number.

[quick check] Do you see that we are arriving at a contradiction here?

Example 1 (2)

Proof. (cont.)

$\neg P$

By definition, we know that a^2 is an even number. From a theorem from last time, we know that a must also be an even number. Again by definition, there exists integer k such that $a = 2k$. We then obtain

$$2b^2 = (2k)^2 = 4k^2,$$

i.e., $b^2 = 2k^2$. This implies that b^2 is an even number. Again, this means that b must be an even number.

[quick check] Do you see that we are arriving at a contradiction here?

(cont. in the next slide) □

Example 1 (3)

Proof. (cont.)

Since a and b are both even numbers, they share 2 as a common factor.

Example 1 (3)

Proof. (cont.)

Since a and b are both even numbers, they share 2 as a common factor. R

This contradicts the fact that we choose the pair a and b that

$\neg R$ share no common factor.

Example 1 (3)

$\neg P$

Proof. (cont.)

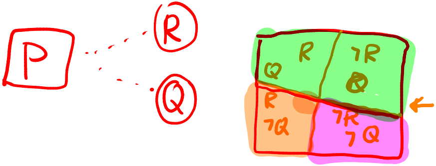
Since a and b are both even numbers, they share 2 as a common factor.

This contradicts the fact that we choose the pair a and b that share no common factor.

Therefore, $\sqrt{2}$ must be irrational. □

$\boxed{P}$

Proofs by cases



- The last proof technique that we shall discuss is closely related to proofs by exhaustion we tried before.
- Sometimes when we want to prove a statement, there are many possible cases. Also, we might not know which cases are true.
- We might still be able to prove the statement if we can show that the statement is true in every case.

Example 2 (1) $\boxed{(n=2)}$ $\boxed{n=3}$

Theorem 2

Suppose that I have 3 pairs of socks: one pair in gray, one pair in white, and one pair in black. If I pick any 4 socks, I will have at least one pair of the same color.

Example 2 (1)

Theorem 2

Suppose that I have 3 pairs of socks: one pair in gray, one pair in white, and one pair in black. If I pick any 4 socks, I will have at least one pair of the same color.

If we want to prove by exhaustion, we will have to consider all 15 cases.

Example 2 (1)

Theorem 2

Suppose that I have 3 pairs of socks: one pair in gray, one pair in white, and one pair in black. If I pick any 4 socks, I will have at least one pair of the same color.

If we want to prove by exhaustion, we will have to consider all 15 cases.

Proof.

Let's split the process of picking 4 socks into 2 steps. First, pick 3 socks, then pick the last sock.

After we pick the first 3 socks. There are 2 possible cases: either I have a pair of socks with the same color, or I do not have such a pair. We shall consider each case separately. P $\neg P$

(cont. in the next slide) □

Example 2 (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*

Example 2 (1)

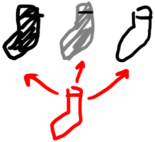
Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true. ✓

Example 2 (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true.
- **Case 2:** *I do not have a pair of socks with the same color.*



Example 2 (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true.
- **Case 2:** *I do not have a pair of socks with the same color.*
  In this case, since I have 3 colors and 3 socks, I must have one sock for each color. Now, after we pick the last sock, whatever color the last one is, we have a color-matching sock in our first 3 socks. Therefore, the theorem is also true in this case.

Example 2 (1)

Proof. (cont.)

- **Case 1:** *I have a pair of socks with the same color.*
  In this case, the theorem is true.
- **Case 2:** *I do not have a pair of socks with the same color.*
  In this case, since I have 3 colors and 3 socks, I must have one sock for each color. Now, after we pick the last sock, whatever color the last one is, we have a color-matching sock in our first 3 socks. Therefore, the theorem is also true in this case.

Since these two cases cover all possibilities, we conclude that the theorem is true. □

Proofs by cases in propositional logic

In propositional logic, the following describe a proof by cases.

$$\begin{array}{l} P \vee Q \vee R \\ P \Rightarrow S \\ Q \Rightarrow S \\ R \Rightarrow S \\ \hline S \end{array}$$

$$\begin{array}{l} P \vee Q \\ P \Rightarrow R \\ Q \Rightarrow R \\ \hline R \end{array}$$

$(P \vee Q) \Rightarrow R$

Proofs by cases in propositional logic

In propositional logic, the following describe a proof by cases.

$$\begin{array}{l} P \vee Q \vee R \\ P \Rightarrow S \\ Q \Rightarrow S \\ R \Rightarrow S \\ \hline S \end{array}$$

Sometimes, when we have 2 cases, we also see:

Proofs by cases in propositional logic

In propositional logic, the following describe a proof by cases.

$$\begin{array}{l} \text{“}P \vee Q \vee R\text{”} \\ P \Rightarrow S \\ Q \Rightarrow S \\ R \Rightarrow S \\ \hline S \end{array}$$

Sometimes, when we have 2 cases, we also see:

$$\begin{array}{l} P \vee \neg P \\ \checkmark\; P \Rightarrow S \\ \checkmark\; \neg P \Rightarrow S \\ \hline \checkmark\; S \end{array}$$

Note that we can leave $\underline{P \vee \neg P}$ out, because it is always true.