

Logic

Discrete Mathematics

Number Theory

Topic 02 — Methods of Mathematical Proof

Mathematical Proofs

Lecture 02 — Proof by Contrapositive and by Cases

Dr Kieran Murphy 

Recurrence Relations

Department of Computing and Mathematics,
Waterford IT.
(kmurphy@wit.ie)

Set Theory

Autumn Semester, 2021

Outline

- Proof by Contrapositive
- Proof by Cases

Enumeration

Outline

1. Proof by Contrapositive 2

- We prove a statement by first switching to the original statement to its contrapositive.

2. Proof by Cases 5

- We prove a statement by breaking it up into smaller and easier cases, which we prove separately.

3. Proof by Contradiction 12

- We prove a statement using the process:
 - assume reverse of statement ...
 - derive conclusions from assumption ...
 - show conclusions are contradictory ...
 - hence assumption must be **False**, so original statement is **True**.

4. Proof by Construction 16

- We prove the existence of something by giving the instructions needed to construct it.

5. Proof by Induction 20

- Special proof technique used to prove a family of statements,

Proof by Contrapositive

Proof by Contrapositive

In a **proof by contrapositive** argument you prove the contrapositive of the claim rather than the claim itself.

Proof by Contrapositive (Formal Structure)

Given claim

$$P \implies Q$$

the contrapositive (and logically equivalent claim) is

$$\neg Q \implies \neg P$$

- 1 Assume $\neg Q$.
- 2 Demonstrate that $\neg P$ must follow from $\neg Q$.

Please, please, . . . , pretty please don't confuse this with proof by contradiction (covered later).

Example

Example 1

If x^2 is odd then x must be odd.

(by contrapositive)*.

The contrapositive is

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

We assume x is even. Hence we can write $x = 2k$ for some integer k . Now

$$x^2 = (2k)^2 = 4k^2 = 2 \underbrace{(2k^2)}_{\substack{\text{integer} \\ \text{even integer}}}$$

Hence the contrapositive is true, and so is the original statement. □

*The above proof is certainly doable by a direct proof. However, a direct proof requires a cumbersome proof by cases approach.

Outline

1. Proof by Contrapositive 2

- We prove a statement by first switching to the original statement to its contrapositive.

2. Proof by Cases 5

- We prove a statement by breaking it up into smaller and easier cases, which we prove separately.

3. Proof by Contradiction 12

- We prove a statement using the process:
 - assume reverse of statement ...
 - derive conclusions from assumption ...
 - show conclusions are contradictory ...
 - hence assumption must be **False**, so original statement is **True**.

4. Proof by Construction 16

- We prove the existence of something by giving the instructions needed to construct it.

5. Proof by Induction 20

- Special proof technique used to prove a family of statements,

Proof by Cases

Proof by Cases

In a **Proof by cases** argument you

- List of of the possible cases and analyse each separately.
- Need to ensure that the cases are exhaustive — cover all possibilities

Proof by Cases (Formal Structure)

Given claim

$$P \implies Q$$

- 1 Show that there exist a number of distinct cases C_1, C_2, \dots such that whenever P is true then at least one of the cases must be true.
- 2 Then, for each case, C , in C_1, C_2, \dots ,
 - 1 Assume case C .
 - 2 Demonstrate that Q must follow from C .

Example 2

I

Example 2

In a cave you find three boxes. One contains gold, the other two are empty. Each box has imprinted on it a clue as to its contents; the clues are:



A: The gold is not here



B: The gold is not here



C: The gold is in box B

Only one message is true; the other two are false. Which box has the gold?

- Notice that I changed the question to “Which box has the gold?”. I could have left it as “Prove that the gold is in box A.” since, for this problem the two versions are equivalent.

Example 2

II

In a proof by cases, there are three cases based on where the gold is located. In each case we check the truth value of the three messages[†]

Gold is in box A

A: “The gold is not here”	F	} Exactly one message true? ✓
B: “The gold is not here”	T	
C: “The gold is in box B”	F	

Gold is in box B

A: “The gold is not here”	T	} Exactly one message true? ✗
B: “The gold is not here”	F	
C: “The gold is in box B”	T	

Gold is in box C

A: “The gold is not here”	T	} Exactly one message true? ✗
B: “The gold is not here”	T	
C: “The gold is in box B”	F	

So in order that exactly one message is true, the gold must be in box A.

[†] You might complain that in the direct proof we did earlier building a truth table is really a proof by cases. You would be correct.

Example 3

Example 3

Every group of 6 minions includes a group of 3 minions who all know each other or a group of 3 minions who are mutual strangers.



Call one of the minions Bob. There are five others. Either Bob knows three of them, or he does not know three of them.

CASE 1: *Bob knows three of the five others ...*

Say that Bob knows three of the five others. Of those five minions either there exists two minions who know each other or no two know each other.

CASE 1.1: *Within the three minions, there exists two who know each other ...*

Then those two and Bob form a mutually acquainted threesome.

CASE 1.2: *No two of the three minions know each other ...*

Then any three of the five minions are a mutually unacquainted threesome.

Example 3

II

CASE 2: *Bob does not know three of the five others ...*

CASE 2.1: *No two of the three minions know each other ...*

Then those two and Bob form a mutually unacquainted threesome.

CASE 2.2: *All pairs within the three minions know each other ...*

Then any three of the five minions are a mutually acquainted threesome.

We have covered all possibilities, and in every instance come up either with a mutually acquainted threesome or a mutually unacquainted threesome.



Examples

- a) Prove that for any integer n , the number $(n^3 - n)$ is even.
- b) Prove that every prime number greater than 3 is either one more or one less than a multiple of 6. Hint. Prove the contrapositive by cases.
- c) Let a, b, c, d be integers. If $a > c$ and $b > c$, then $\max(a, b) - c$ is always positive.