VANDERBILT UNIVERSITY School of Engineering

Discrete Structures

CS 2212

(Fall 2020)

6 – Proofs

Reminder and Recap …

Reminders:

- **ZyBook Assig. 2A** due **Sep 13** (11:59 PM)
- **Exam 1** on **Sep 17** (Thursday)
- **HW 1** due **Sep 22** (Tuesday)

Exam 1:

- Exam 1 will be at Brightspace.
- Exam 1 will be during class time.
- Practice quiz on Brightspace. (I will upload solutions also)
- Formula sheet is available at Brightspace (Course Resources Folder)
- Office Hours on Tuesday for the sake of exam. (next week only)

Chapter 2

Proofs

- We have developed necessary machinery and toolset to start proving theorems involving numbers.
- We will see some more proof techniques now.

Proofs - Introduction

Theorem

Fact/given + Fact/given → New fact

Proving a Theorem

Proofs - Introduction

Theorem

Fact/given + Fact/given → New fact

Proving a Theorem

Fact/given

Fact/given

Proofs - Introduction

Theorem

Fact/given + Fact/given → New fact

Proving a Theorem

Fact/given

Fact/given

New fact

Proofs - Introduction

Theorem

Fact/given + Fact/given → New fact

Proving a Theorem

Fact/given

Fact/given

New fact

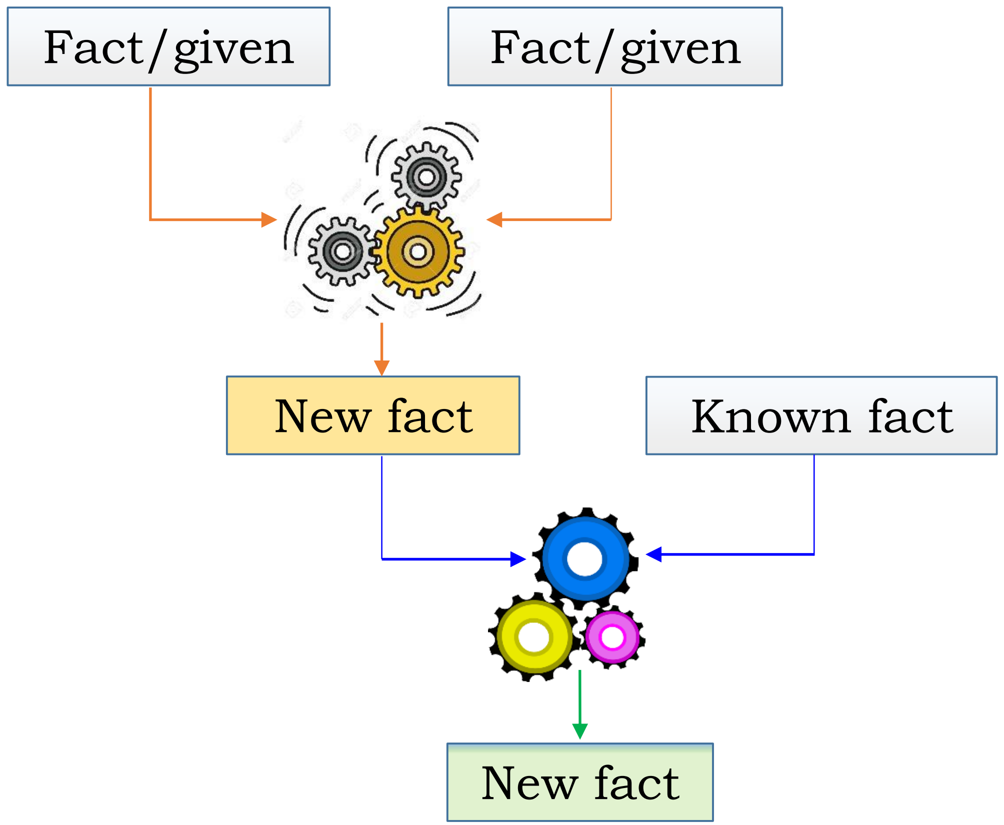
Known fact

Proofs - Introduction

Theorem

Fact/given + Fact/given → New fact

Proving a Theorem

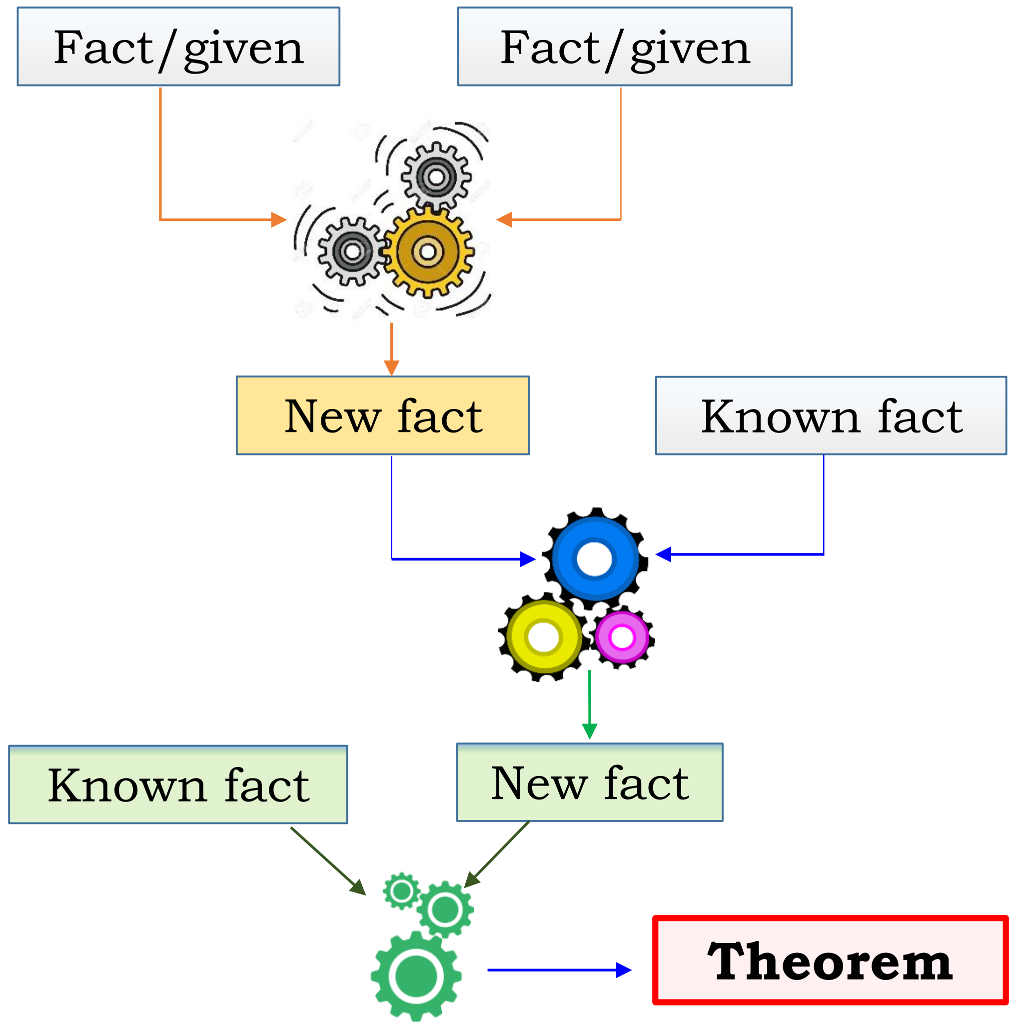


Proofs - Introduction

Theorem

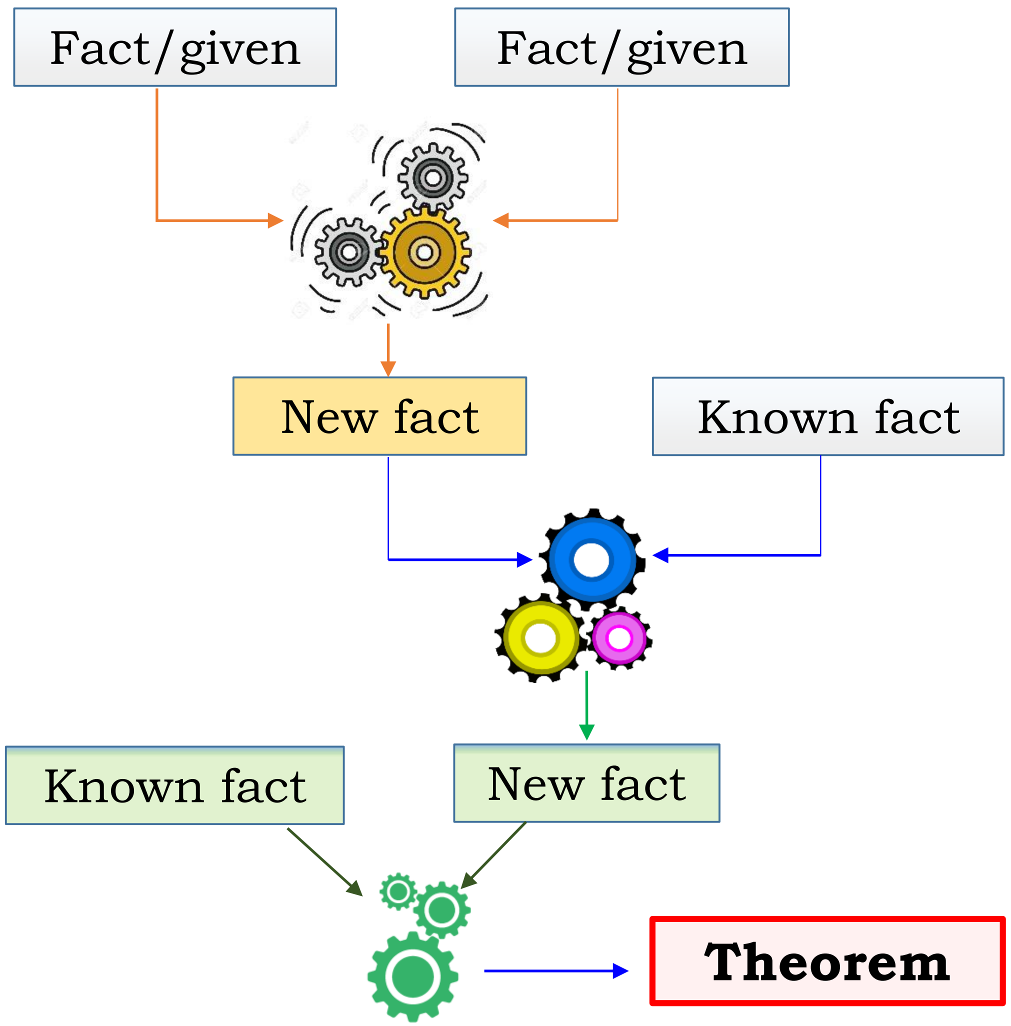
Fact/given + Fact/given → New fact

Proving a Theorem



Proofs - Introduction

Proving a Theorem



Important Considerations while Proving

- What do we know?
- What else do we need to know?
- How can we "combine" known facts to get new information.
- Which (mathematical) tools should we apply, and when should we apply them?
- …

No fixed approach/method

Its a "creative art" and a skill

Proof Techniques

- We will see various “approaches” and “techniques” to proving theorems.
- We will try to prove statements involving numbers and more.
- Chapter 1 (Logic) has set up the foundation to move forward.

- Proofs by exhaustion
- Direct proofs
- Proofs by contrapositive
- Proofs by contradiction
- Proofs by cases

Some Definitions

Natural numbers	**N**	0, 1, 2, …
Integers	**Z**	…, -2, -1, 0, 1, 2, …
Positive integers	$\mathbf{Z}^+$	1, 2, 3, …
Rational numbers	**Q**	$\frac{n}{m}$ with $n \in \mathbf{Z}$ and $m \in \mathbf{Z}^+$
Irrational numbers		real number that cannot be written as a simple fraction
Even integers		Integers that have the form $\mathbf{2}\boldsymbol{k}$ for some integer k
Odd integers		Integers that have the form $\mathbf{2}\boldsymbol{k}\mathbf{+1}$ for some integer k

Some Definitions

Divisibility:

Symbol: $m \mid n$

Reads: m divides n

Definition: if $m \neq 0$ and $n = km$ for some integer k

Example: $3 \mid 6$

Important properties of divisibility:

- If $d|a$ and $a|b$ then $d|b$
- If $d|a$ and $a|b$ then $d|(xa + yb)$ for any integers x, y

Some Definitions

Prime number An integer n is prime if and only if $n > 1$, and for every positive integer m, if $m \mid n$, then $m = 1$ or $m = n$.

Composite number An integer n is composite if and only if $n > 1$, and there is an integer $1 < m < n$ such that $m \mid n$.

Parity The number is odd or even.

Same Parity If two numbers are both even or both odd.

Opposite Parity If one number is odd and the other is even.

Proofs - Exhaustive Checking

- **What:** This technique works by checking every possibility in the testing domain.
- **When to use:**
  - Works well if you only have to perform a small number of tests (e.g., x is an integer such that $3 \le x \le 6$).
  - Does not work well with a large domain (e.g., All politicians are liars).
- **Difficulty:** Easy to use but it will get cumbersome as the domain to test gets larger (kind of like truth tables).

Proofs - Exhaustive Checking

Example: Prove that the numbers in the set **{288, 198, 387}** are divisible by **9**.

Proof by exhaustive checking:

1. By definition $\boldsymbol{m \mid n}$ if $\boldsymbol{m \neq 0}$ and $\boldsymbol{n = km}$ for some integer k.
2. Let n be values in the set {288, 198, 387} and let $m = 9$.
3. For $n = 288$ and $m = 9$ we have $k = 32$.
4. Therefore 288 is divisible by 9.
5. For $n = 198$ and $m = 9$ we have $k = 22$.
6. Therefore 198 is divisible by 9.
7. For $n = 387$ and $m = 9$ we have $k = 43$.
8. Therefore 387 is divisible by 9.
9. We can conclude that 288, 198 and 387 are all divisible by 9.
10. QED

Proofs

While writing proofs, keep the following in mind:

- Clarity
- Precision
- Conciseness

Tips:

- Don't skip or assume steps.
- Justify every step.
- Clearly articulate your reasoning.
- Avoid circular reasoning
- (See Section 2.3 of the book)

Proofs

Circular Reasoning

Using the fact to be proven in the proof itself.

If an integer n is odd then n^2 is odd

Proof:

- If n is an odd integer, then $n = 2k+1$ for some integer k.
- Let $n^2 = 2j + 1$ for some integer j.
- Since n^2 is equal to two times an integer plus 1, then n^2 is odd.

Direct Proofs

Many statements we need to prove are **conditionals** (i.e., if X is even, then X^2 is even).

We have seen the flavor of this approach in the first chapter.

The process is as follows:

1. **Assume the antecedent** is true.
2. **Find statement(s) that follow** from this assumption and/or known facts.
3. Continue until the **consequent** is reached.
4. As long as the consequent is also **true**, we have sufficiently proved what we wanted.

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.
Then, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.
Then, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.
Then, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
Since k is integer, $(2k^2 + 2k)$ is also an integer. Lets say $m = 2k^2 + 2k$

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.
Then, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
Since k is integer, $(2k^2 + 2k)$ is also an integer. Lets say $m = 2k^2 + 2k$
Thus, $x^2 = 2m + 1$, for an integer m.

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.
Then, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
Since k is integer, $(2k^2 + 2k)$ is also an integer. Lets say $m = 2k^2 + 2k$
Thus, $x^2 = 2m + 1$, for an integer m.
Thus, x^2 must be an odd integer by definition.

Direct Proofs

Prove: If x is an odd integer, then x^2 is also an odd integer.

(Before start writing the proof, lets think about our plan of action.)

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.
Then, $x^2 = (2k + 1)^2 \ = 4k^2 + 4k + 1$
$= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
Since k is integer, $(2k^2 + 2k)$ is also an integer. Lets say $m = 2k^2 + 2k$
Thus, $x^2 = 2m + 1$, for an integer m.
Thus, x^2 must be an odd integer by definition.
QED.

Direct Proofs

Prove:

For any positive real numbers, x and y,

$$x + y \geq \sqrt{xy}$$

Direct Proofs

Prove:

If n and m are both perfect square integers, then nm is also a perfect square integer.

Proofs by Contraposition

Proof by contrapositive

A proof by contrapositive proves a conditional theorem of the form $P \rightarrow Q$ by showing that the contrapositive $\neg Q \rightarrow \neg P$ is true.

Proofs by Contraposition

Prove: If x^2 is an even integer, then x is an even integer.

P: x^2 is an even integer

Q: x is an even integer

Proofs by Contraposition

Prove: If x^2 is an even integer, then x is an even integer.

P: x^2 is an even integer

Q: x is an even integer

Our approach:

We need to show $P \rightarrow Q$.

But, we know if $P \rightarrow Q$, then $\neg Q \rightarrow \neg P$.

So, lets try proving $\neg Q \rightarrow \neg P$. (may be its easy).

Proofs by Contraposition

Prove: If x^2 is an even integer, then x is an even integer.

P: x^2 is an even integer

Q: x is an even integer

Our approach:

We need to show $P \rightarrow Q$.

But, we know if $P \rightarrow Q$, then $\neg Q \rightarrow \neg P$.

So, lets try proving $\neg Q \rightarrow \neg P$. (may be its easy).

Prove: If x is an odd integer, then x^2 is an odd integer.

Proofs by Contraposition

Prove: If x is an odd integer, then x^2 is an odd integer.

So, we can just **copy** our old proof.

Proofs by Contraposition

Prove: If x is an odd integer, then x^2 is an odd integer.

So, we can just **copy** our old proof.

Assume x is an odd integer.
Since x is odd, $x = 2k + 1$ for some integer k.
Then, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
Since k is integer, $(2k^2 + 2k)$ is also an integer. Lets say $m = 2k^2 + 2k$
Thus, $x^2 = 2m + 1$, for an integer m.
Thus, x^2 must be an odd integer by definition.
QED.

Proofs by Contraposition

Prove: If 3x+2 is odd, then x is odd

P: 3x+2 is odd

Q: x is odd

We need to show: $P \rightarrow Q$

Proofs by Contraposition

Prove: If 3x+2 is odd, then x is odd

P: 3x+2 is odd

Q: x is odd

We need to show: $P \rightarrow Q$

Lets try a **direct approach** first.

1.	3x+2 is odd.	Premise
2.	3x+2 = 2k+1	By the definition of odd numbers
3.	????	???

Proofs by Contraposition

Prove: If $3x+2$ is odd, then x is odd

P: $3x+2$ is odd

Q: x is odd

We need to show: $P \rightarrow Q$

Lets try a **direct approach** first.

1. $3x+2$ is odd.	Premise
2. $3x+2 = 2k+1$	By the definition of odd numbers
3. ????	???

There does not seem to be a direct way to conclude from here that n is odd. Lets try our new approach using contraposition

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

1.	x is even	Given

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

1.	x is even	Given
2.	$x = 2k$ for some k	By the definition of even numbers

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

1.	x is even	Given
2.	$x = 2k$ for some k	By the definition of even numbers
3.	Thus, $3x+2 = 3(2k) + 2$	Replacing x in $(3x+2)$

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

1.	x is even	Given
2.	$x = 2k$ for some k	By the definition of even numbers
3.	Thus, $3x+2 = 3(2k) + 2$	Replacing x in $(3x+2)$
4.	$3(2k) + 2 = 2(3k)+2$	Simplifying line 3

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

1.	x is even	Given
2.	$x = 2k$ for some k	By the definition of even numbers
3.	Thus, $3x+2 = 3(2k) + 2$	Replacing x in $(3x+2)$
4.	$3(2k) + 2 = 2(3k)+2$	Simplifying line 3
5.	$2(3k)+2 = 2(3k+1)$ is even	By the definition of even numbers

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

1. x is even	Given
2. x = 2k for some k	By the definition of even numbers
3. Thus, 3x+2 = 3(2k) + 2	Replacing x in (3x+2)
4. 3(2k) + 2 = 2(3k)+2	Simplifying line 3
5. 2(3k)+2 = 2(3k+1) is even	By the definition of even numbers
6. Thus, 3x+2 is an even	From line 5

Proofs by Contraposition

Prove: If x is an even, then 3x+2 is even.

(We are showing: $\neg Q \rightarrow \neg P$)

1.	x is even	Given
2.	x = 2k for some k	By the definition of even numbers
3.	Thus, 3x+2 = 3(2k) + 2	Replacing x in (3x+2)
4.	3(2k) + 2 = 2(3k)+2	Simplifying line 3
5.	2(3k)+2 = 2(3k+1) is even	By the definition of even numbers
6.	Thus, 3x+2 is an even	From line 5
7.	QED.	

Now, using contrapositive, we have shown that

If 3x+2 is odd, then x is odd

Proofs by Contraposition

Prove:

For $x \in Z$, if $7x+9$ is even, then x is odd.

Lets try to prove it directly first.

Next, lets prove it using contraposition.

Proofs – By Contradiction

General Approach:

1. Suppose the statement to be proved is false, that is, suppose that the negation of the statement is true.
2. Show that this supposition leads logically to a contradiction.
3. Conclude that the statement to be proved is true.

Proofs – By Contradiction

General Approach:

We need to show $P \rightarrow Q$.

Assume $\neg Q$.

contradiction

Then, we show that $(P \land \neg Q) \rightarrow \boxed{(r \land \neg r)}$ for some statement r.

Why this approach works?

- We showed that $P \land \neg Q$ is always false (as it leads to a contradiction).
- Since P is given and is true, so $\neg Q$ must be false.
- That means Q is true, which is the desired statement.

Proofs – By Contradiction

General Approach:

We need to show $P \to Q$.

Assume $\neg Q$.

Then, we show that $(P \land \neg Q) \to (r \land \neg r)$ for some proposition r.

- Do you see any similarity / difference with the **proof by contraposition?**
- Which one is more general?
- Proof by contradiction is a very useful approach.

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

(Assuming negation of the given statement)
Assume there is at least one integer n that is both even and odd.

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

(Assuming negation of the given statement) Assume there is at least one integer n that is both even and odd.
(Now try to deduce a contradiction) Thus, n = 2a for some integer a (by the definition of even integer)

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

(Assuming negation of the given statement) Assume there is at least one integer n that is both even and odd.
(Now try to deduce a contradiction) Thus, $n = 2a$ for some integer a (by the definition of even integer)
Similarly, $n = 2b + 1$ for some integer b (by the definition of odd)

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

(Assuming negation of the given statement) Assume there is at least one integer n that is both even and odd.
(Now try to deduce a contradiction) Thus, $n = 2a$ for some integer a (by the definition of even integer)
Similarly, $n = 2b + 1$ for some integer b (by the definition of odd)
Consequently, $2a = 2b + 1$

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

(Assuming negation of the given statement) Assume there is at least one integer n that is both even and odd.
(Now try to deduce a contradiction) Thus, $n = 2a$ for some integer a (by the definition of even integer)
Similarly, $n = 2b + 1$ for some integer b (by the definition of odd)
Consequently, $2a = 2b + 1$
And so, $2a - 2b = 1$
$2(a - b) = 1$
$a - b = 1/2$

Proofs – By Contradiction

Prove: There is no integer that is both even and odd.

(Assuming negation of the given statement) Assume there is at least one integer n that is both even and odd.
(Now try to deduce a contradiction) Thus, $n = 2a$ for some integer a (by the definition of even integer)
Similarly, $n = 2b + 1$ for some integer b (by the definition of odd)
Consequently, $2a = 2b + 1$
And so, $2a - 2b = 1$
$2(a - b) = 1$
$a - b = 1/2$
Since, a and b are integers, their difference must be integer. But, here $(a - b)$ is not an integer, which is a contradiction. Hence, the given statement is true.

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement)
Assume there is rational number r and an irrational number i such that their sum is rational.

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)
And, $r + i = \frac{c}{d}$, for some c and d (by our assumption)

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)
And, $r + i = \frac{c}{d}$, for some c and d (by our assumption)
So, $\frac{a}{b} + i = \frac{c}{d}$

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)
And, $r + i = \frac{c}{d}$, for some c and d (by our assumption)
So, $\frac{a}{b} + i = \frac{c}{d}$
$i = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)
And, $r + i = \frac{c}{d}$, for some c and d (by our assumption)
So, $\frac{a}{b} + i = \frac{c}{d}$
$i = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$
Since a,b,c,d are integers, $(bc - ad)$ is an integer and bd is also an integer. Moreover, $bd \neq 0$ (by the zero product property).

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)
And, $r + i = \frac{c}{d}$, for some c and d (by our assumption)
So, $\frac{a}{b} + i = \frac{c}{d}$
$i = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$
Since a,b,c,d are integers, $(bc - ad)$ is an integer and bd is also an integer. Moreover, $bd \neq 0$ (by the zero product property).
This means that i is a rational number, which is a contradiction.

Proofs – By Contradiction

Prove: The sum of any rational number and any irrational number is irrational.

(Assuming negation of the given statement) Assume there is rational number r and an irrational number i such that their sum is rational.
(Now try to deduce a contradiction) $r = \frac{a}{b}$, for some a and b (by the definition of rational numbers)
And, $r + i = \frac{c}{d}$, for some c and d (by our assumption)
So, $\frac{a}{b} + i = \frac{c}{d}$
$i = \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$
Since a,b,c,d are integers, $(bc - ad)$ is an integer and bd is also an integer. Moreover, $bd \neq 0$ (by the zero product property).
This means that i is a rational number, which is a contradiction.
Thus, the given statement is true.

Proofs – By Contradiction

Prove:

$\sqrt{2}$ is an irrational number

Proofs – By Contradiction

Prove:

There is no greatest integer.