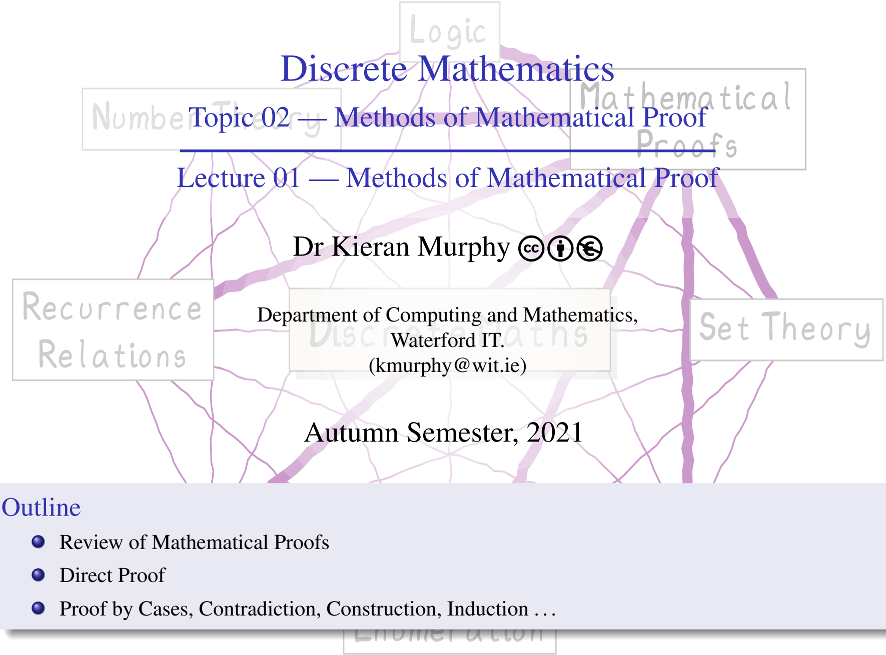


Discrete Mathematics

Topic 02 — Methods of Mathematical Proof

Lecture 01 — Methods of Mathematical Proof

Dr Kieran Murphy

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

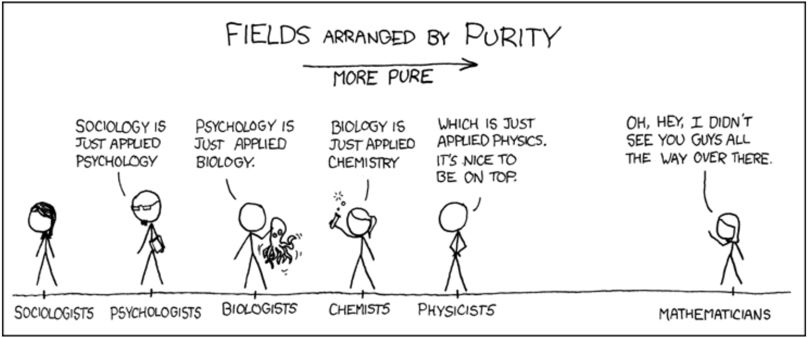
Autumn Semester, 2021

Outline

- Review of Mathematical Proofs
- Direct Proof
- Proof by Cases, Contradiction, Construction, Induction . . .

Why do we Need Proofs?

Mathematics is perhaps the only field in which absolute certainty is possible.


FIELDS ARRANGED BY PURITY
MORE PURE
SOCIOLOGY IS JUST APPLIED PSYCHOLOGY
PSYCHOLOGY IS JUST APPLIED BIOLOGY.
BIOLOGY IS JUST APPLIED CHEMISTRY
WHICH IS JUST APPLIED PHYSICS. IT'S NICE TO BE ON TOP.
OH, HEY, I DIDN'T SEE YOU GUYS ALL THE WAY OVER THERE.
SOCIOLOGISTS
PSYCHOLOGISTS
BIOLOGISTS
CHEMISTS
PHYSICISTS
MATHEMATICIANS

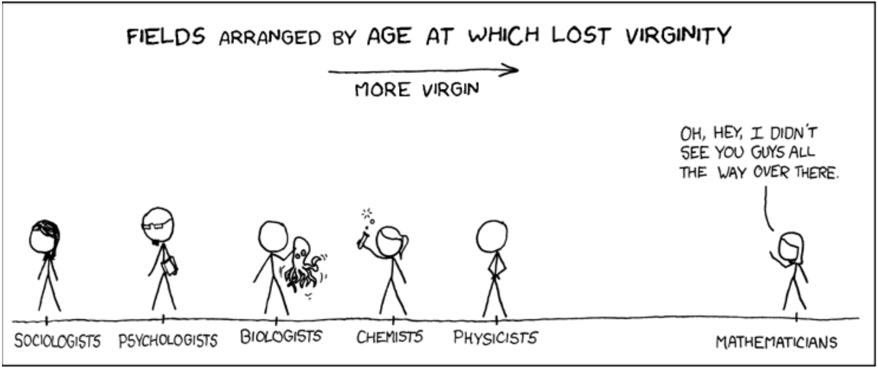
This certainty come with a price — it takes effort and patience.

> *For God's sake, I beseech you, give it up. Fear it no less than sensual passions and because it, too, may take all your time, and deprive you of your health, peace of mind and happiness in life.*
>
> — *mathematician Farkas Bolyai (1775–1856) advice to his son to stay away from mathematics.*

https://xkcd.com/435

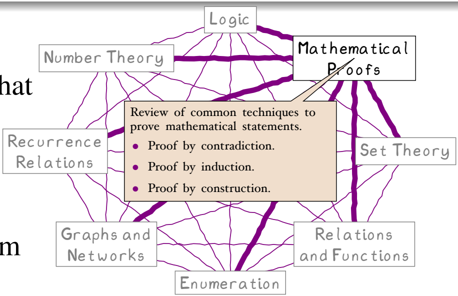
An aside …

Other professions' response to Mathematicians' boasts of certainty …


FIELDS ARRANGED BY AGE AT WHICH LOST VIRGINITY
MORE VIRGIN
OH, HEY, I DIDN'T SEE YOU GUYS ALL THE WAY OVER THERE.
SOCIOLOGISTS
PSYCHOLOGISTS
BIOLOGISTS
CHEMISTS
PHYSICISTS
MATHEMATICIANS

Motivation for Focusing on Techniques

Regardless of the area of Discrete Mathematics or the type of problem that we are studying we often have claims that we want to either prove or disprove.



Review of common techniques to prove mathematical statements.

- Proof by contradiction.
- Proof by induction.
- Proof by construction.

The utility of Mathematics comes from the fact that

While the area/problem may vary the techniques remain the same.

Main Techniques

- Proof by Contradiction

  Assume the negative of the claim and show that this leads to a contradiction.
- Proof by Cases

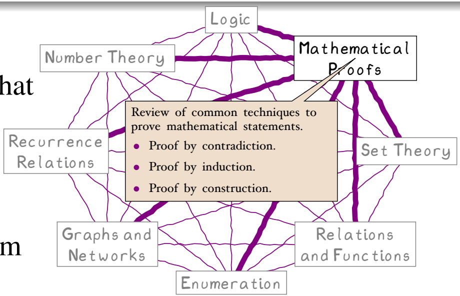
  List all possibilities (case) and analyse each separably.
- Proof by Construction, Direct Proof, . . .

Often a proof is a mixture of techniques.

Motivation for Focusing on Techniques

Regardless of the area of Discrete Mathematics or the type of problem that we are studying we often have claims that we want to either prove or disprove.

The utility of Mathematics comes from the fact that



Logic

Mathematical Proofs

Number Theory

Recurrence Relations

Set Theory

Graphs and Networks

Relations and Functions

Enumeration

Review of common techniques to prove mathematical statements.

- Proof by contradiction.
- Proof by induction.
- Proof by construction.

While the area/problem may vary the techniques remain the same.

Main Techniques

- Proof by Contradiction

  Assume the negative of the claim and show that this leads to a contradiction.
- Proof by Cases

  List all possibilities (case) and analyse each separably.
- Proof by Construction, Direct Proof, . . .

Often a proof is a mixture of techniques.

Some Miscellaneous Mathematical Facts I

Properties of Integers

- The negative of an integer is an integer.
- The sum, difference and product of two integers is an integer.
- An integer, n, is even if $n = 2k$ for some integer k.
- An integer, n, is odd if $n = 2k + 1$ for some integer k.
- Any real number, x, can be written as a sum of an integer x_n, and a fractional part, x_f, where $0 \leq x_f < 1$.

$$x = \underbrace{x_n}_{\substack{\text{integer}\\ \text{part}}} + \underbrace{x_f}_{\substack{\text{fractional}\\ \text{part}\\ 0 \leq x_f < 1}}$$

- The floor function, denoted by $\text{floor}(x) = \lfloor x \rfloor$ returns the largest integer less than or equal to x, i.e., the integer part of x.
- The ceiling function, denoted by $\text{ceil}(x) = \lceil x \rceil$ returns the smallest integer greater than or equal to x.

Some Miscellaneous Mathematical Facts I

Properties of Integers

- The negative of an integer is an integer.
- The sum, difference and product of two integers is an integer.
- An integer, n, is even if $n = 2k$ for some integer k.
- An integer, n, is odd if $n = 2k + 1$ for some integer k.
- Any real number, x, can be written as a sum of an integer x_n, and a fractional part, x_f, where $0 \leq x_f < 1$.

$$x = \underbrace{x_n}_{\substack{\text{integer}\\ \text{part}}} + \underbrace{x_f}_{\substack{\text{fractional}\\ \text{part}\\ 0 \leq x_f < 1}}$$

- The floor function, denoted by $\text{floor}(x) = \lfloor x \rfloor$ returns the largest integer less than or equal to x, i.e., the integer part of x.
- The ceiling function, denoted by $\text{ceil}(x) = \lceil x \rceil$ returns the smallest integer greater than or equal to x.

Some Miscellaneous Mathematical Facts I

Properties of Integers

- The negative of an integer is an integer.
- The sum, difference and product of two integers is an integer.
- An integer, n, is even if $n = 2k$ for some integer k.
- An integer, n, is odd if $n = 2k + 1$ for some integer k.
- Any real number, x, can be written as a sum of an integer x_n, and a fractional part, x_f, where $0 \leq x_f < 1$.

$$x = \underbrace{x_n}_{\substack{\text{integer}\\ \text{part}}} + \underbrace{x_f}_{\substack{\text{fractional}\\ \text{part}\\ 0 \leq x_f < 1}}$$

- The floor function, denoted by $\text{floor}(x) = \lfloor x \rfloor$ returns the largest integer less than or equal to x, i.e., the integer part of x.
- The ceiling function, denoted by $\text{ceil}(x) = \lceil x \rceil$ returns the smallest integer greater than or equal to x.

Some Miscellaneous Mathematical Facts I

Properties of Integers

- The negative of an integer is an integer.
- The sum, difference and product of two integers is an integer.
- An integer, n, is even if $n = 2k$ for some integer k.
- An integer, n, is odd if $n = 2k + 1$ for some integer k.
- Any real number, x, can be written as a sum of an integer x_n, and a fractional part, x_f, where $0 \leq x_f < 1$.

$$x = \underbrace{x_n}_{\substack{\text{integer}\\\text{part}}} + \underbrace{x_f}_{\substack{\text{fractional}\\\text{part}\\0 \leq x_f < 1}}$$

- The floor function, denoted by $\text{floor}(x) = \lfloor x \rfloor$ returns the largest integer less than or equal to x, i.e., the integer part of x.
- The ceiling function, denoted by $\text{ceil}(x) = \lceil x \rceil$ returns the smallest integer greater than or equal to x.

Some Miscellaneous Mathematical Facts II

The floor and ceiling functions can be confusing, especially for negative integers[*]

x	integer part, x_n	fractional part, x_f	$\text{floor}(x) = \lfloor x \rfloor$	$\text{ceil}(x) = \lceil x \rceil$
7	7	0	7	7
7.2	7	0.2	7	8
7.9	7	0.9	7	8
-7.9	-8	0.1	-8	-7
-7.2	-8	0.8	-8	-7
-7	-7	0	-7	-7

The important things to remember are :

- The fractional part is always zero (for integers) or positive.
- The ceiling is equal to the floor for integers.
- The ceiling is equal to the floor plus one for non-integers.

[*] Microsoft Excel had implemented the ceiling function incorrectly up until Excel 2010.

Some Miscellaneous Mathematical Facts II

The floor and ceiling functions can be confusing, especially for negative integers[*]

x	integer part, x_n	fractional part, x_f	$\text{floor}(x) = \lfloor x \rfloor$	$\text{ceil}(x) = \lceil x \rceil$
7	7	0	7	7
7.2	7	0.2	7	8
7.9	7	0.9	7	8
-7.9	-8	0.1	-8	-7
-7.2	-8	0.8	-8	-7
-7	-7	0	-7	-7

The important things to remember are :

- The fractional part is always zero (for integers) or positive.
- The ceiling is equal to the floor for integers.
- The ceiling is equal to the floor plus one for non-integers.

[*] Microsoft Excel had implemented the ceiling function incorrectly up until Excel 2010.

Types of Mathematical Statements

Theorems

Very important statements that have many and varied consequences.

Propositions

Less important and consequential statements.

Corollaries

Statements for which the truth can be deduced almost immediately from other statements.

Lemmas

Statements that don’t have much intrinsic interest but help to prove other theorems.

Outline

1. Direct Proof 8
   - We use the premises in the problem to show that the claim must be true.
2. Proof by Contrapositive 16
   - We prove a statement by first switching to the original statement to its contrapositive.
3. Proof by Cases 19
   - We prove a statement by breaking it up into smaller and easier cases, which we prove separately.
4. Proof by Contradiction 26
   - 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**.
5. Proof by Construction 30
   - We prove the existence of something by giving the instructions needed to construct it.
6. Proof by Induction 34
   - Special proof technique used to prove a family of statements,

Direct Proof

Direct Proof

In a direct proof argument you apply the given premises to show that the claim must be correct.

Direct Proof (Formal Structure)

Given claim

$$P \implies Q$$

You

1. Assume P.
2. Demonstrate that Q must follow from P.

Example 1 I

Example 1

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. Prove that the gold is in box A.

Note: The claim, may often be expressed as a question, e.g., "Is the gold in box A?", "Where is the gold?" etc.

Example 1 II

A direct proof here, would be to formalise the problem in propositional logic and find the solution using properties of logical operators (or using a truth table).

(Atomic) Propositions

- A = "*Gold is in box A*"
- B = "*Gold is in box B*"
- C = "*Gold is in box C*"

Statements (Not premises since, we don't asumme their truth value)

- S_1 = "*Gold is not here*" (box A message)

$$S_1 = \neg A$$

- S_2 = "*Gold is not here*" (box B message)

$$S_2 = \neg B$$

- S_3 = "*Gold is in box B*" (box C message)

$$S_3 = B$$

Example 1 II

A direct proof here, would be to formalise the problem in propositional logic and find the solution using properties of logical operators (or using a truth table).

(Atomic) Propositions

- A = "*Gold is in box A*"
- B = "*Gold is in box B*"
- C = "*Gold is in box C*"

Statements (Not premises since, we don't asumme their truth value)

- S_1 = "*Gold is not here*" (box A message)

$$S_1 = \neg A$$

- S_2 = "*Gold is not here*" (box B message)

$$S_2 = \neg B$$

- S_3 = "*Gold is in box B*" (box C message)

$$S_3 = B$$

Example 1 II

A direct proof here, would be to formalise the problem in propositional logic and find the solution using properties of logical operators (or using a truth table).

(Atomic) Propositions

- A = "*Gold is in box A*"
- B = "*Gold is in box B*"
- C = "*Gold is in box C*"

Statements (Not premises since, we don't asumme their truth value)

- S_1 = "*Gold is not here*" (box A message)

$$S_1 = \neg A$$

- S_2 = "*Gold is not here*" (box B message)

$$S_2 = \neg B$$

- S_3 = "*Gold is in box B*" (box C message)

$$S_3 = B$$

Example 1 III

Premises

- P_1 = "*One box contains gold, the other two are empty.*"

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or } \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- P_2 = "*Only one message is true; the other two are false*"

(messages are S_1, S_2 and S_3)

$$P_2 = (S_1 \wedge \neg S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge \neg S_2 \wedge S_3)$$

Example 1 III

Premises

- $P_1 =$ *"One box contains gold, the other two are empty."*

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or } \dots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- $P_2 =$ *"Only one message is true; the other two are false"*

(messages are S_1, S_2 and S_3)

$$P_2 = (S_1 \wedge \neg S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge \neg S_2 \wedge S_3)$$

Example 1 III

Premises

- P_1 = "*One box contains gold, the other two are empty.*"

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or} \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- P_2 = "*Only one message is true; the other two are false*"

(messages are S_1, S_2 and S_3)

$$P_2 = (S_1 \wedge \neg S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge \neg S_2 \wedge S_3)$$

Example 1 III

Premises

- $P_1 =$ "*One box contains gold, the other two are empty.*"

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or} \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- $P_2 =$ "*Only one message is true; the other two are false*"

(messages are S_1, S_2 and S_3)

$$P_2 = (S_1 \wedge \neg S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge \neg S_2 \wedge S_3)$$

Example 1 III

Premises

- $P_1 =$ "*One box contains gold, the other two are empty.*"

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or} \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- $P_2 =$ "*Only one message is true; the other two are false*"

(messages are S_1, S_2 and S_3)

$$P_2 = \left(S_1 \wedge \neg S_2 \wedge \neg S_3\right) \vee \left(\neg S_1 \wedge S_2 \wedge \neg S_3\right) \vee \left(\neg S_1 \wedge \neg S_2 \wedge S_3\right)$$

Example 1 III

Premises

- $P_1 =$ "*One box contains gold, the other two are empty.*"

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or} \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- $P_2 =$ "*Only one message is true; the other two are false*"

(messages are S_1, S_2 and S_3)

$$P_2 = (S_1 \wedge \neg S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge \neg S_2 \wedge S_3)$$

$\boxed{S_1 = \neg A, S_2 = \neg B, S_3 = B}$

$$= (\neg A \wedge \neg\neg B \wedge \neg B) \vee (\neg\neg A \wedge \neg B \wedge \neg B) \vee (\neg\neg A \wedge \neg\neg B \wedge B)$$

Example 1 III

Premises

- P_1 = "*One box contains gold, the other two are empty.*"

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or} \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- P_2 = "*Only one message is true; the other two are false*"

(messages are S_1, S_2 and S_3)

$$P_2 = (S_1 \wedge \neg S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge \neg S_2 \wedge S_3)$$

$\boxed{S_1 = \neg A, S_2 = \neg B, S_3 = B}$

$$= (\neg A \wedge \neg\neg B \wedge \neg B) \vee (\neg\neg A \wedge \neg B \wedge \neg B) \vee (\neg\neg A \wedge \neg\neg B \wedge B)$$

$\boxed{\neg\neg p = p}$

$$= (\neg A \wedge B \wedge \neg B) \vee (A \wedge \neg B \wedge \neg B) \vee (A \wedge B \wedge B)$$

Example 1 III

Premises

- $P_1 =$ "*One box contains gold, the other two are empty.*"

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or } \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- $P_2 =$ "*Only one message is true; the other two are false*"

(messages are S_1, S_2 and S_3)

$$P_2 = \left(S_1 \wedge \neg S_2 \wedge \neg S_3\right) \vee \left(\neg S_1 \wedge S_2 \wedge \neg S_3\right) \vee \left(\neg S_1 \wedge \neg S_2 \wedge S_3\right)$$

$\boxed{S_1 = \neg A, S_2 = \neg B, S_3 = B}$

$$= \left(\neg A \wedge \neg\neg B \wedge \neg B\right) \vee \left(\neg\neg A \wedge \neg B \wedge \neg B\right) \vee \left(\neg\neg A \wedge \neg\neg B \wedge B\right)$$

$\boxed{\neg\neg p = p}$

$$= \left(\neg A \wedge B \wedge \neg B\right) \vee \left(A \wedge \neg B \wedge \neg B\right) \vee \left(A \wedge B \wedge B\right)$$

$\boxed{p \wedge \neg p = \mathbf{F}}$

$$= \left(\mathbf{F}\right) \vee \left(A \wedge \neg B\right) \vee \left(A \wedge B\right)$$

Example 1 III

Premises

- $P_1 =$ *"One box contains gold, the other two are empty."*

$$P_1 = \underbrace{(A \wedge \neg B \wedge \neg C)}_{\text{in A and not in B and not in C or} \ldots} \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$$

- $P_2 =$ *"Only one message is true; the other two are false"*

(messages are S_1, S_2 and S_3)

$$P_2 = (S_1 \wedge \neg S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge S_2 \wedge \neg S_3) \vee (\neg S_1 \wedge \neg S_2 \wedge S_3)$$

$\boxed{S_1 = \neg A, S_2 = \neg B, S_3 = B}$

$$= (\neg A \wedge \neg\neg B \wedge \neg B) \vee (\neg\neg A \wedge \neg B \wedge \neg B) \vee (\neg\neg A \wedge \neg\neg B \wedge B)$$

$\boxed{\neg\neg p = p}$

$$= (\neg A \wedge B \wedge \neg B) \vee (A \wedge \neg B \wedge \neg B) \vee (A \wedge B \wedge B)$$

$\boxed{p \wedge \neg p = \mathbf{F}}$

$$= (\mathbf{F}) \vee (A \wedge \neg B) \vee (A \wedge B)$$

$$= (A \wedge \neg B) \vee (A \wedge B)$$

Example 1 IV

The claim "*Gold is in box A*" is equivalent to show the proposition

$$P_1 \wedge P_2 \rightarrow A$$

as a tautology. We could do this using the properties of logical operators, or we can construct a truth table

- $P_1 = (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$
- $P_2 = (A \wedge \neg B) \vee (A \wedge B)$

A	B	C	P_1	P_2	$P_1 \wedge P_2 \rightarrow A$
F	**F**	**F**	**F**	**F**	**T**
F	**F**	**T**	**T**	**F**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**T**	**T**	**F**	**F**	**T**
T	**F**	**F**	**T**	**T**	**T**
T	**F**	**T**	**F**	**T**	**T**
T	**T**	**F**	**F**	**T**	**T**
T	**T**	**T**	**F**	**T**	**T**

Example 1 IV

The claim "*Gold is in box A*" is equivalent to show the proposition

$$P_1 \land P_2 \rightarrow A$$

as a tautology. We could do this using the properties of logical operators, or we can construct a truth table

- $P_1 = (A \land \neg B \land \neg C) \lor (\neg A \land B \land \neg C) \lor (\neg A \land \neg B \land C)$
- $P_2 = \big(A \land \neg B\big) \lor \big(A \land B\big)$

A	B	C	P_1	P_2	$P_1 \land P_2 \rightarrow A$
F	**F**	**F**	**F**	**F**	**T**
F	**F**	**T**	**T**	**F**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**T**	**T**	**F**	**F**	**T**
T	**F**	**F**	**T**	**T**	**T**
T	**F**	**T**	**F**	**T**	**T**
T	**T**	**F**	**F**	**T**	**T**
T	**T**	**T**	**F**	**T**	**T**

Example 1 IV

The claim “*Gold is in box A*” is equivalent to show the proposition

$$P_1 \wedge P_2 \rightarrow A$$

as a tautology. We could do this using the properties of logical operators, or we can construct a truth table

- $P_1 = (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$
- $P_2 = \big(A \wedge \neg B\big) \vee \big(A \wedge B\big)$

A	B	C	P_1	P_2	$P_1 \wedge P_2 \rightarrow A$
F	**F**	**F**	**F**	**F**	**T**
F	**F**	**T**	**T**	**F**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**T**	**T**	**F**	**F**	**T**
T	**F**	**F**	**T**	**T**	**T**
T	**F**	**T**	**F**	**T**	**T**
T	**T**	**F**	**F**	**T**	**T**
T	**T**	**T**	**F**	**T**	**T**

(premises true implies conclusion true)

Example 1

The claim "*Gold is in box A*" is equivalent to show the proposition

$$P_1 \wedge P_2 \to A$$

as a tautology. We could do this using the properties of logical operators, or we can construct a truth table

- $P_1 = (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$
- $P_2 = \big(A \wedge \neg B\big) \vee \big(A \wedge B\big)$

A	B	C	P_1	P_2	$P_1 \wedge P_2 \to A$
F	**F**	**F**	**F**	**F**	**T**
F	**F**	**T**	**T**	**F**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**T**	**T**	**F**	**F**	**T**
T	**F**	**F**	**T**	**T**	**T**
T	**F**	**T**	**F**	**T**	**T**
T	**T**	**F**	**F**	**T**	**T**
T	**T**	**T**	**F**	**T**	**T**

(premises true implies conclusion true)

Hence the claim is true and the gold is in box A.

Example 1 IV

The claim *"Gold is in box A"* is equivalent to show the proposition

$$P_1 \land P_2 \to A$$

as a tautology. We could do this using the properties of logical operators, or we can construct a truth table

- $P_1 = (A \land \neg B \land \neg C) \lor (\neg A \land B \land \neg C) \lor (\neg A \land \neg B \land C)$
- $P_2 = \big(A \land \neg B\big) \lor \big(A \land B\big)$

A	B	C	P_1	P_2	$P_1 \land P_2 \to A$
F	**F**	**F**	**F**	**F**	**T**
F	**F**	**T**	**T**	**F**	**T**
F	**T**	**F**	**T**	**F**	**T**
F	**T**	**T**	**F**	**F**	**T**
T	**F**	**F**	**T**	**T**	**T**
T	**F**	**T**	**F**	**T**	**T**
T	**T**	**F**	**F**	**T**	**T**
T	**T**	**T**	**F**	**T**	**T**

(premises true implies conclusion true)

We could have saved some work and only wrote rows for which P_1 was true, i.e., exactly one of A, B, and C are **T**.

Hence the claim is true and the gold is in box A.

Example 2

Example 2

Let a and b be consecutive integers. Then, show that $a+b$ is odd.

Proof (Direct Proof).

Since a and b are consecutive integers, we can assume without loss of generality that $a=b+1$. Then, we have

$$a+b=(b+1)+b=\underbrace{\underbrace{2b}_{\text{even}}+1}_{\text{odd}}$$

Therefore, $a+b$ is odd. □

Example 2

Example 2

Let a and b be consecutive integers. Then, show that $a + b$ is odd.

Proof (Direct Proof).

Since a and b are consecutive integers, we can assume without loss of generality that $a = b + 1$. Then, we have

$$a + b = (b + 1) + b = \underbrace{\underbrace{2b}_{\text{even}} + 1}_{\text{odd}}$$

Therefore, $a + b$ is odd. □

Examples

a) The sum of two odd numbers is even.

b) The product of two odd numbers is odd.

c) The square of an even natural number is even.

d) If A and B are real positive numbers, then

$$\underbrace{\frac{A+B}{2}}_{\text{arithmetic mean}} \geq \underbrace{\sqrt{AB}}_{\text{geometric mean}}$$

Hint: Use fact that $(a-b)^2 = a^2 - 2ab + b^2 \geq 0$.

e) Prove the Pythagorean theorem.

f) Prove that $x = y$ if and only if $xy = \frac{(x+y)^2}{4}$. Note, you will need to prove in two “directions” here: the “if” and the “only if” part.

Outline

1. Direct Proof 8
   - We use the premises in the problem to show that the claim must be true.

2. Proof by Contrapositive 16
   - We prove a statement by first switching to the original statement to its contrapositive.

3. Proof by Cases 19
   - We prove a statement by breaking it up into smaller and easier cases, which we prove separately.

4. Proof by Contradiction 26
   - 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**.

5. Proof by Construction 30
   - We prove the existence of something by giving the instructions needed to construct it.

6. Proof by Induction 34
   - 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 3

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

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

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.

Example

Example 3

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

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

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. Direct Proof 8
   - We use the premises in the problem to show that the claim must be true.

2. Proof by Contrapositive 16
   - We prove a statement by first switching to the original statement to its contrapositive.

3. Proof by Cases 19
   - We prove a statement by breaking it up into smaller and easier cases, which we prove separately.

4. Proof by Contradiction 26
   - 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**.

5. Proof by Construction 30
   - We prove the existence of something by giving the instructions needed to construct it.

6. Proof by Induction 34
   - 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 $C_1, C_2, \ldots$ such that whenever P is true then at least one of the cases must be true.
2. Then, for each case, C, in $C_1, C_2, \ldots$,
    1. Assume case C.
    2. Demonstrate that Q must follow from C.

Example 4 I

Example 4

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 4 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

Gold is in box B

Gold is in box C

[‡] 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 4 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*"
B: "*The gold is not here*"
C: "*The gold is in box B*"

Gold is in box B

A: "*The gold is not here*"
B: "*The gold is not here*"
C: "*The gold is in box B*"

Gold is in box C

A: "*The gold is not here*"
B: "*The gold is not here*"
C: "*The gold is in box B*"

[‡] 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 4 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**
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*”
B: “*The gold is not here*”
C: “*The gold is in box B*”

Gold is in box C

A: “*The gold is not here*”
B: “*The gold is not here*”
C: “*The gold is in box B*”

[‡] 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 4 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**

B: “*The gold is not here*” **T**

C: “*The gold is in box B*” **F**

} Exactly one message true? ✔

Gold is in box B

A: “*The gold is not here*”

B: “*The gold is not here*”

C: “*The gold is in box B*”

Gold is in box C

A: “*The gold is not here*”

B: “*The gold is not here*”

C: “*The gold is in box B*”

[‡] 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 4 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**
B: "*The gold is not here*" **T**
C: "*The gold is in box B*" **F**

Exactly one message true? ✔

Gold is in box B

A: "*The gold is not here*" **T**
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*"
B: "*The gold is not here*"
C: "*The gold is in box B*"

[‡] 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 4 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*"

B: "*The gold is not here*"

C: "*The gold is in box B*"

[‡] 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 4 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**
B: "*The gold is not here*"	**T**
C: "*The gold is in box B*"	**F**

[‡] 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 4 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**	

[‡] 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 4 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 5 I

Example 5

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: *There exists two minions who know each other …*

Then those two and Bob form a mutually acquainted threesome.

CASE 1.2: *No two of the five minions know each other …*

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

Example 5

I

Example 5

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: *There exists two minions who know each other . . .*

Then those two and Bob form a mutually acquainted threesome.

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

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

Example 5 I

Example 5

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: *There exists two minions who know each other . . .*

Then those two and Bob form a mutually acquainted threesome.

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

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

Example 5 I

Example 5

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: *There exists two minions who know each other …*

Then those two and Bob form a mutually acquainted threesome.

CASE 1.2: *No two of the five minions know each other …*

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

Example 5

Example 5

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: *There exists two minions who know each other . . .*

Then those two and Bob form a mutually acquainted threesome.

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

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

Example 5 II

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

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

Then those two and Bob form a mutually unacquainted threesome.

CASE 2.2: *All pairs within the five 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.

Example 5 II

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

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

Then those two and Bob form a mutually unacquainted threesome.

CASE 2.2: *All pairs within the five 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.

Example 5 II

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

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

Then those two and Bob form a mutually unacquainted threesome.

CASE 2.2: *All pairs within the five 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.

Example 5 II

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

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

Then those two and Bob form a mutually unacquainted threesome.

CASE 2.2: *All pairs within the five 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.

Outline

1. Direct Proof 8

- We use the premises in the problem to show that the claim must be true.

2. Proof by Contrapositive 16

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

3. Proof by Cases 19

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

4. Proof by Contradiction 26

- 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**.

5. Proof by Construction 30

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

6. Proof by Induction 34

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

Proof by Contradiction I

Proof by Contradiction

In a proof by contradiction argument you:

- Assume the negative of the claim
  - So a universal claim will become an existence claim, and an existence claim will become a universal claim.
- Then show that the assumption leads to a contradiction.

Proof by Contradiction (Formal Structure)

Given claim

$$P \implies Q$$

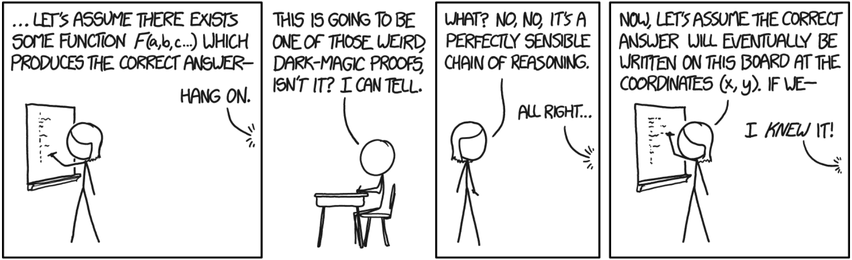
Show that the negative, i.e. $P \Rightarrow \neg Q$, leads to a contradiction, by

1. Assume P.
2. Assume $\neg Q$.
3. Use P and $\neg Q$ to demonstrate a contradiction.

Proof by Contradiction II

Proofs by contradiction can be tricky, you

- Need to be very clear as to what statement you are assuming in order to generate a contradiction.
- In particular, take case when the statement involves a qualifier.


... LET'S ASSUME THERE EXISTS SOME FUNCTION F(a,b,c...) WHICH PRODUCES THE CORRECT ANSWER–
HANG ON.
THIS IS GOING TO BE ONE OF THOSE WEIRD, DARK-MAGIC PROOFS, ISN'T IT? I CAN TELL.
WHAT? NO, NO, IT'S A PERFECTLY SENSIBLE CHAIN OF REASONING.
ALL RIGHT...
NOW, LET'S ASSUME THE CORRECT ANSWER WILL EVENTUALLY BE WRITTEN ON THIS BOARD AT THE COORDINATES (x, y). IF WE–
I KNEW IT!

[§] https://xkcd.com/1724/

Examples

a) Prove that a triangle cannot have more than one right angle.

b) Prove that the $\sqrt{2}$ is irrational.[¶]

c) Prove that $\log_2(3)$ is irrational.

d) Let n be an integer. If $3n + 2$ is odd, then n is odd.

e) Prove that there are an infinite number of primes.[‖]

f) There are no integers x and y such that $x^2 = 4y + 2$.

g) The Pigeonhole Principle: If more than n pigeons fly into n pigeon holes, then at least one pigeon hole will contain at least two pigeons. Prove this.

[¶] “irrational”= “not rational”. A rational number is a number that can be expressed as quotient of two integers p and p which don’t have a common factor.

[‖] A prime is an integer greater than one with exactly two divisors.

Outline

1. Direct Proof 8
    - We use the premises in the problem to show that the claim must be true.
2. Proof by Contrapositive 16
    - We prove a statement by first switching to the original statement to its contrapositive.
3. Proof by Cases 19
    - We prove a statement by breaking it up into smaller and easier cases, which we prove separately.
4. Proof by Contradiction 26
    - 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**.
5. Proof by Construction 30
    - We prove the existence of something by giving the instructions needed to construct it.
6. Proof by Induction 34
    - Special proof technique used to prove a family of statements,

Proof by Construction

Proof by Construction

In a proof by construction argument you:

- Are dealing with an existence claim.
- Prove existence of an object by actually constructing it.
- The proof usually involves stating the steps (algorithm) needed to construct the required object.

- This type of proof is more powerful than just an existence proof — this not only proves existence but also create an example.
- Very common in geometry, and graph theory

Example 6

Example 6

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 6

Example 6

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow\quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow}\quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow\quad & ar + b = as + b \\ \Longrightarrow\quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow}\quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 6

Example 6

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & & ar + b &= 0 \\ &\Longrightarrow & ar &= -b \\ &\overset{a \neq 0}{\Longrightarrow} & r &= -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & & ar + b = 0 &= as + b \\ &\Longrightarrow & ar + b &= as + b \\ &\Longrightarrow & ar &= as \\ &\overset{a \neq 0}{\Longrightarrow} & r &= s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 6

Example 6

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a \neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a \neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 6

Example 6

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \implies \quad & ar = -b \\ \overset{a\neq 0}{\implies} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \implies \quad & ar + b = as + b \\ \implies \quad & ar = as \\ \overset{a\neq 0}{\implies} \quad & r = s \end{aligned}$$

Contradiction! $\implies$ $r = s$ is unique. □

Example 6

Example 6

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow \quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow \quad & ar + b = as + b \\ \Longrightarrow \quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow} \quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Example 6

Example 6

If a and b are real numbers and $a \neq 0$, then there exists a unique r such that

$$ar + b = 0$$

Here we have two claims: existence and uniqueness.

Existence (by construction).

Construction

$$\begin{aligned} & ar + b = 0 \\ \Longrightarrow\quad & ar = -b \\ \overset{a\neq 0}{\Longrightarrow}\quad & r = -b/a \end{aligned}$$

Verify

$$ar + b = a\left(\frac{-b}{a}\right) + b = -b + b = 0$$

Construction: $r = -b/a$ □

Uniqueness (by contradiction).

Assume there are two values, r and s, with $r \neq s$ satisfying the equation. Then

$$\begin{aligned} & ar + b = 0 = as + b \\ \Longrightarrow\quad & ar + b = as + b \\ \Longrightarrow\quad & ar = as \\ \overset{a\neq 0}{\Longrightarrow}\quad & r = s \end{aligned}$$

Contradiction! $\Longrightarrow$ $r = s$ is unique. □

Examples

a) Prove that x^n can be computed using only $\log_2(n)$ multiplications when n is a power of 2.

This is a special case of the Montgomery algorithm for computing large integer power quickly — a big deal in cryptography!

b) Prove that the sum of the first n positive integers equals $n(n+1)/2$

Outline

1. Direct Proof 8

- We use the premises in the problem to show that the claim must be true.

2. Proof by Contrapositive 16

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

3. Proof by Cases 19

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

4. Proof by Contradiction 26

- 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**.

5. Proof by Construction 30

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

6. Proof by Induction 34

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

Proof by Induction

Proof by Induction

A proof by induction argument, can be applied when Q, the conclusion in the claim $P \Rightarrow Q$, can be represented as a sequence of related claims, $Q_1, Q_2, Q_3, \ldots$. Then we show, that

- the first claim is true, and
- if any claim is true, then the next claim must also be true.

Proof by Induction (Formal Structure)

Given family of claims, where integer n is 1,2,3,4,. . . ,

$$P \Rightarrow Q_n$$

1. Assume P, (now we need to prove that all of $Q_1, Q_2, Q_3, \ldots$, are true)
2. Prove Q_1. (the basic/initial step)
3. Prove $Q_k \Rightarrow Q_{k+1}$ for arbitrary integer k. (the inductive step)**

**Instead of attacking the problem directly, we only explain how to get a proof for Q_{k+1} when given a proof for Q_k.

Example 7 I

Example 7

Suppose an ATM has only twenty euro and fifty euro bills. You can type in the amount you want, and it will figure out how to divide things up into the proper number of twenty and fifty euro bills.

Prove that the ATM can generate any multiple of 10 euro amount ≥ 40.

(by induction).

First we define the proposition (or family of propositions)

$$Q_n : \text{ATM can output } 10n \text{ euro} = 20a + 50b$$

where a and b are nonnegative integers

We want to prove the sequence

$$Q_4, Q_5, Q_6, \ldots$$

Note: In this example we did not start at one (and our stride was 10). □

Example 7 I

Example 7

Suppose an ATM has only twenty euro and fifty euro bills. You can type in the amount you want, and it will figure out how to divide things up into the proper number of twenty and fifty euro bills.

Prove that the ATM can generate any multiple of 10 euro amount ≥ 40.

(by induction).

First we define the proposition (or family of propositions)

$$Q_n : \text{ATM can output } 10n \text{ euro} = 20a + 50b$$

where a and b are nonnegative integers

We want to prove the sequence

$$Q_4, Q_5, Q_6, \ldots$$

Note: In this example we did not start at one (and our stride was 10). □

Example 7 II

Q_n : $10n = 20a + 50b$ where a and b are nonnegative integers

the basis step, Q_4

$$10(4) \overset{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 7 II

$$Q_n : \quad 10n = 20a + 50b \qquad \text{where } a \text{ and } b \text{ are nonnegative integers}$$

the basis step, Q_4

$$10(4) \overset{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 7 II

$$Q_n : \quad 10n = 20a + 50b \qquad \text{where } a \text{ and } b \text{ are nonnegative integers}$$

the basis step, Q_4

$$10(4) \overset{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 7 II

$$Q_n : \quad 10n = 20a + 50b \qquad \text{where } a \text{ and } b \text{ are nonnegative integers}$$

the basis step, Q_4

$$10(4) \overset{?}{=} 20a + 50b \qquad \textbf{True} \quad a = 2, b = 0$$

i.e., ATM can output forty euro by outputting two twenty euro and no fifty euro notes.

the inductive step

Assume Q_k. It is equivalent to assuming

$$10k = 20a + 50b \quad \text{for some non-negative integers } a \text{ and } b$$

i.e., ATM can output $10k$ euro by outputting only twenty euro and fifty euro notes.

and now we want to prove Q_{k+1}, ie,

$$10(k+1) = 20A + 50B \quad \text{for some non-negative integers } A \text{ and } B$$

i.e., ATM can output $10(k+1)$ euro by outputting only twenty euro and fifty euro notes.

Example 7 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Example 7 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

Hence $b > 0$, To get ten more euro out we replace one fifty by three twenties, i.e.,

$$10k = 20a + 50b \implies 10k + 10 = 10(k+1) = 20(a+3) + 50\underbrace{(b-1)}_{\text{OK, since } b > 0}$$

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Example 7 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

Hence $b > 0$, To get ten more euro out we replace one fifty by three twenties, i.e.,

$$10k = 20a + 50b \implies 10k + 10 = 10(k+1) = 20(a+3) + 50\underbrace{(b-1)}_{\text{OK, since } b > 0}$$

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Hence $a \geq 2$, since $10k \geq 40$. To get ten more euro out we replace two twenties by one fifty, i.e.,

$$10k = 20a + 50(0) \implies 10k + 10 = 10(k+1) = 20\underbrace{(a-2)}_{\text{OK, since } a > 2} + 50(1)$$

Example 7 III

To prove Q_{k+1} we have two cases:

CASE 1: *The ATM used at least one fifty when outputting* $10k$ *euro.*

Hence $b > 0$, To get ten more euro out we replace one fifty by three twenties, i.e.,

$$10k = 20a + 50b \implies 10k + 10 = 10(k+1) = 20(a+3) + 50\underbrace{(b-1)}_{\text{OK, since } b > 0}$$

CASE 1: *The ATM used no fifty euro notes when outputting* $10k$ *euro.*

Hence $a \geq 2$, since $10k \geq 40$. To get ten more euro out we replace two twenties by one fifty, i.e.,

$$10k = 20a + 50(0) \implies 10k + 10 = 10(k+1) = 20\underbrace{(a-2)}_{\text{OK, since } a > 2} + 50(1)$$

We have proven the two steps required in an induction argument, hence we can conclude the sequence of claims are true.

Examples

a) For all integers n, prove that $n^2 + 5n + 6$ is even.

b) Prove that the sum of the first n positive integers equals $n(n+1)/2$

c) Prove for integer $n \geq 4$, that $3^n > 2n^2 + 3n$.