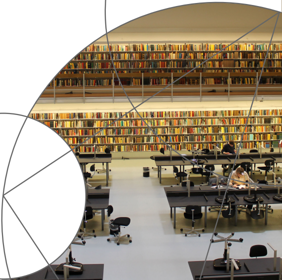
DMA: Proofs

Laura Mančinska
Institut for Matematiske Fag



Outline

- Proof method: case analysis

Outline

- Proof method: case analysis
- To prove or to disprove?

Outline

- Proof method: case analysis
- To prove or to disprove?
- The axiomatic method
- “The blue-eyed islanders”

Proof by case analysis

Task: Prove q

Proof by case analysis

Task: Prove q

Proof template

- Write: "We use case analysis."

Proof by case analysis

Task: Prove q

Proof template

- Write: "We use case analysis."
- Identify a list of conditions, at least one of which must hold.

  (If it is not obvious that the list is exhaustive, you must prove it.)

Proof by case analysis

Task: Prove q

Proof template

- Write: "We use case analysis."
- Identify a list of conditions, at least one of which must hold.

  (If it is not obvious that the list is exhaustive, you must prove it.)
- For each condition:
  - State the condition.
  - Prove q assuming that the condition holds.

Proof by case analysis (example)

Task: Prove that in every set S of 6 people there are

- at least 3 mutual strangers OR
- at least 3 mutual friends.

Proof by case analysis (example)

Task: Prove that in every set S of 6 people there are

- at least 3 mutual strangers OR
- at least 3 mutual friends.

Proof. Let $\mathcal{A}$ be a set of six people and $\mathrm{P} \in \mathcal{A}$ be one of them. We analyze cases:

Proof by case analysis (example)

Task: Prove that in every set S of 6 people there are

- at least 3 mutual strangers OR
- at least 3 mutual friends.

Proof. Let $\mathcal{A}$ be a set of six people and $P \in \mathcal{A}$ be one of them. We analyze cases:

1. P has at least 3 (different) friends $F_1, F_2, F_3 \in \mathcal{A}$.
2. P is stranger to at least 3 (different) people $S_1, S_2, S_3 \in \mathcal{A}$.

Proof by case analysis (example)

Task: Prove that in every set S of 6 people there are

- at least 3 mutual strangers OR
- at least 3 mutual friends.

Proof. Let $\mathcal{A}$ be a set of six people and $P \in \mathcal{A}$ be one of them. We analyze cases:

1. P has at least 3 (different) friends $F_1, F_2, F_3 \in \mathcal{A}$.
2. P is stranger to at least 3 (different) people $S_1, S_2, S_3 \in \mathcal{A}$.

Q: Why is the list exhaustive?

(finish on the board)

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.
    - True (we proved it on Tuesday).

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.
   - True (we proved it on Tuesday).
2. For all $x, y \in \mathbb{R}$, $(x = y) \Leftrightarrow (x^2 = y^2)$.

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.
   - True (we proved it on Tuesday).
2. For all $x, y \in \mathbb{R}$, $(x = y) \Leftrightarrow (x^2 = y^2)$.
   - Not true. Why?

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.
   - True (we proved it on Tuesday).
2. For all $x, y \in \mathbb{R}$, $(x = y) \Leftrightarrow (x^2 = y^2)$.
   - Not true. Why?
3. Let $a, b, d \in \mathbb{Z}^+$. If $d \mid (ab)$, then $d \mid a$ or $d \mid b$.

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.
   - True (we proved it on Tuesday).
2. For all $x, y \in \mathbb{R}$, $(x = y) \Leftrightarrow (x^2 = y^2)$.
   - Not true. Why?
3. Let $a, b, d \in \mathbb{Z}^+$. If $d \mid (ab)$, then $d \mid a$ or $d \mid b$.
   - Not true. Why?

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.
   - True (we proved it on Tuesday).
2. For all $x, y \in \mathbb{R}$, $(x = y) \Leftrightarrow (x^2 = y^2)$.
   - Not true. Why?
3. Let $a, b, d \in \mathbb{Z}^+$. If $d \mid (ab)$, then $d \mid a$ or $d \mid b$.
   - Not true. Why?

An x which invalidates "$\forall x \in S\ P(x)$" is called a counterexample.

To prove or to disprove?

Sometimes we don't know whether a statement q is true or not.

1. If $x, y \in \mathbb{Z}$ are odd, then $x + y$ is even.
   - True (we proved it on Tuesday).
2. For all $x, y \in \mathbb{R}$, $(x = y) \Leftrightarrow (x^2 = y^2)$.
   - Not true. Why?
3. Let $a, b, d \in \mathbb{Z}^+$. If $d \mid (ab)$, then $d \mid a$ or $d \mid b$.
   - Not true. Why?

An x which invalidates "$\forall x \in S\ P(x)$" is called a counterexample.
To disprove a "for all"-type statement, we only need a counterexample.

The axiomatic method

In 300 BC Euclid invented the axiomatic method for establishing the truth of a statement.

The axiomatic method

In 300 BC Euclid invented the axiomatic method for establishing the truth of a statement.

- Postulate a number of axioms.

The axiomatic method

In 300 BC Euclid invented the axiomatic method for establishing the truth of a statement.

- Postulate a number of axioms.
- Prove new statements from axioms and previously proven statements.

The axiomatic method

In 300 BC Euclid invented the axiomatic method for establishing the truth of a statement.

- Postulate a number of axioms.
- Prove new statements from axioms and previously proven statements.

Proof is a a sequence of logical deductions (valid arguments).

Warm-up

- Assume, we have shown that an implication

$$p \Rightarrow q$$

is a true statement.

Warm-up

- Assume, we have shown that an implication

$$p \Rightarrow q$$

  is a true statement.
- **Q:** Can we conclude that q is a true statement?

Warm-up

- Assume, we have shown that an implication

  $$p \Rightarrow q$$

  is a true statement.
- **Q:** Can we conclude that q is a true statement?
- **A: No!** When we prove that $(p \Rightarrow q)$ is true, we don't show that q is true, but that

  if p is true, *then* q is true.

Warm-up

- Assume, we have shown that an implication

$$p \Rightarrow q$$

  is a true statement.
- **Q:** Can we conclude that q is a true statement?
- **A: No!** When we prove that $(p \Rightarrow q)$ is true, we don't show that q is true, but that

  if p is true, *then* q is true.

- **Q:** What additional assumption do we need, to conclude that q is true?

Warm-up

- **Assume**, we have shown that an implication

$$p \Rightarrow q$$

  is a true statement.
- **Q:** Can we conclude that q is a true statement?
- **A: No!** When we prove that $(p \Rightarrow q)$ is true, we don't show that q is true, but that

  if p is true, *then* q is true.

- **Q:** What additional assumption do we need, to conclude that q is true?
- Indeed, $(p \wedge (p \Rightarrow q)) \Rightarrow q$ is a tautology (check!).

Logical deductions

Def. Given logical statements $p_1, \ldots, p_n$ and q, we say that q logically follows from $p_1, \ldots, p_n$ if

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q \quad \text{is a tautology.}$$

Logical deductions

Def. Given logical statements $p_1, \ldots, p_n$ and q, we say that q logically follows from $p_1, \ldots, p_n$ if

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q \quad \text{is a tautology.}$$

Notation:

$$\begin{array}{rll} & p_1 & \\ & p_2 & \text{Hypotheses} \\ & \vdots & \\ & p_n & \\ \hline \therefore & q & \text{Conclusion} \end{array}$$

Logical deductions

Def. Given logical statements $p_1, \ldots, p_n$ and q, we say that q logically follows from $p_1, \ldots, p_n$ if

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow q \quad \text{is a tautology.}$$

Notation:

$$\begin{array}{rll} & p_1 & \\ & p_2 & \text{Hypotheses} \\ & \vdots & \\ & p_n & \\ \hline \therefore & q & \text{Conclusion} \end{array}$$

Example (modus ponens)

$$\begin{array}{l} p \\ p \Rightarrow q \\ \hline q \end{array}$$

On Tuesday...

We proved that for any $a \in \mathbb{Z}$:

$$(a \text{ is even}) \Leftrightarrow (a^2 \text{ is even})$$

On Tuesday...

We proved that for any $a \in \mathbb{Z}$:

$$(a \text{ is even}) \Leftrightarrow (a^2 \text{ is even})$$

We also proved that $\sqrt{2}$ is irrational via proof by contradiction:

- Assume (for contradiction) that $\sqrt{2}$ is rational, *i.e.* $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}^+$, where $\gcd(a, b) = 1$.
- Then $2 = \frac{a^2}{b^2}$.

On Tuesday...

We proved that for any $a \in \mathbb{Z}$:

$$(a \text{ is even}) \Leftrightarrow (a^2 \text{ is even})$$

We also proved that $\sqrt{2}$ is irrational via proof by contradiction:

- Assume (for contradiction) that $\sqrt{2}$ is rational, *i.e.* $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}^+$, where $\gcd(a, b) = 1$.
- Then $2 = \frac{a^2}{b^2}$. So $a^2 = 2b^2$

On Tuesday...

We proved that for any $a \in \mathbb{Z}$:

$$(a \text{ is even}) \Leftrightarrow (a^2 \text{ is even})$$

We also proved that $\sqrt{2}$ is irrational via proof by contradiction:

- Assume (for contradiction) that $\sqrt{2}$ is rational, *i.e.* $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}^+$, where $\gcd(a, b) = 1$.
- Then $2 = \frac{a^2}{b^2}$. So $a^2 = 2b^2$ which shows that a^2 is even.

On Tuesday...

We proved that for any $a \in \mathbb{Z}$:

$$(a \text{ is even}) \Leftrightarrow (a^2 \text{ is even})$$

We also proved that $\sqrt{2}$ is irrational via proof by contradiction:

- Assume (for contradiction) that $\sqrt{2}$ is rational, *i.e.* $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}^+$, where $\gcd(a, b) = 1$.
- Then $2 = \frac{a^2}{b^2}$. So $a^2 = 2b^2$ which shows that a^2 is even.

So we had established that

$$a^2 \text{ is even} \qquad \wedge \qquad ((a^2 \text{ is even}) \Rightarrow (a \text{ is even}))$$

On Tuesday...

We proved that for any $a \in \mathbb{Z}$:

$$(a \text{ is even}) \Leftrightarrow (a^2 \text{ is even})$$

We also proved that $\sqrt{2}$ is irrational via proof by contradiction:

- Assume (for contradiction) that $\sqrt{2}$ is rational, *i.e.* $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}^+$, where $\gcd(a, b) = 1$.
- Then $2 = \frac{a^2}{b^2}$. So $a^2 = 2b^2$ which shows that a^2 is even.

So we had established that

$$a^2 \text{ is even} \qquad \wedge \qquad ((a^2 \text{ is even}) \Rightarrow (a \text{ is even}))$$

Then we concluded that a must be even. This was modus ponens.

A logical deduction?

Example.

If today is Wednesday, then Mette has POP today.

Today is not Wednesday.

Mette does not have POP today.

A logical deduction?

Example.

If today is Wednesday, then Mette has POP today.

Today is not Wednesday.

Mette does not have POP today.

Not a valid argument, since

$$((p \Rightarrow q) \wedge (\sim p)) \Rightarrow (\sim q)$$

is *not* a tautology. (When does it fail to be true?)

A logical deduction?

Example.

If I cycle to university, then I arrive tired.

I did not arrive tired.

I did not cycle to university.

A logical deduction?

Example.

If I cycle to university, then I arrive tired.

I did not arrive tired.

I did not cycle to university.

Valid argument, since

$$((p \Rightarrow q) \wedge (\sim q)) \Rightarrow (\sim p)$$

is a tautology (check!).

Let's "prove" that $1/8 > 1/4$

Bogus proof

$$\begin{aligned} 3 &> 2 && \Leftrightarrow \\ 3\log_{10}(1/2) &> 2\log_{10}(1/2) && \Leftrightarrow \\ \log_{10}(1/2)^3 &> \log_{10}(1/2)^2 && \Leftrightarrow \\ (1/2)^3 &> (1/2)^2 \end{aligned}$$

$\square$

Let's "prove" that $1/8 > 1/4$

Bogus proof

$$\begin{aligned} 3 &> 2 && \Leftrightarrow \\ 3\log_{10}(1/2) &> 2\log_{10}(1/2) && \Leftrightarrow \\ \log_{10}(1/2)^3 &> \log_{10}(1/2)^2 && \Leftrightarrow \\ (1/2)^3 &> (1/2)^2 \end{aligned}$$

$\square$

What's wrong here?

A common mistake

Let $a, b \in \mathbb{R}^+$. It is a fact that the Arithmetic Mean is at least as large as the Geometric Mean, namely,

$$\frac{a+b}{2} \geqslant \sqrt{ab}$$

A common mistake

Let $a, b \in \mathbb{R}^+$. It is a fact that the Arithmetic Mean is at least as large as the Geometric Mean, namely,

$$\frac{a+b}{2} \geqslant \sqrt{ab}$$

Bogus proof

$$\begin{aligned} \frac{a+b}{2} &\geqslant \sqrt{ab} && \text{so} \\ a+b &\geqslant 2\sqrt{ab} && \text{so} \\ a^2+2ab+b^2 &\geqslant 4ab && \text{so} \\ a^2-2ab+b^2 &\geqslant 0 && \text{so} \\ (a-b)^2 &\geqslant 0 && \text{which we know is true.} \end{aligned}$$

A common mistake

Let $a, b \in \mathbb{R}^+$. It is a fact that the Arithmetic Mean is at least as large as the Geometric Mean, namely,

$$\frac{a+b}{2} \geqslant \sqrt{ab}$$

Bogus proof

$$\begin{aligned} \frac{a+b}{2} &\geqslant \sqrt{ab} && \text{so} \\ a+b &\geqslant 2\sqrt{ab} && \text{so} \\ a^2+2ab+b^2 &\geqslant 4ab && \text{so} \\ a^2-2ab+b^2 &\geqslant 0 && \text{so} \\ (a-b)^2 &\geqslant 0 && \text{which we know is true.} \end{aligned}$$

So we have shown that $(a+b)/2 \geqslant \sqrt{ab}$. □

A common mistake

Let $a, b \in \mathbb{R}^+$. It is a fact that the Arithmetic Mean is at least as large as the Geometric Mean, namely,

$$\frac{a+b}{2} \geqslant \sqrt{ab}$$

Bogus proof

$$\begin{aligned} \frac{a+b}{2} &\geqslant \sqrt{ab} && \text{so} \\ a+b &\geqslant 2\sqrt{ab} && \text{so} \\ a^2+2ab+b^2 &\geqslant 4ab && \text{so} \\ a^2-2ab+b^2 &\geqslant 0 && \text{so} \\ (a-b)^2 &\geqslant 0 && \text{which we know is true.} \end{aligned}$$

So we have shown that $(a+b)/2 \geqslant \sqrt{ab}$. □

What is wrong here and how can we fix it?

A common mistake

Let $a, b \in \mathbb{R}^+$. It is a fact that the Arithmetic Mean is at least as large as the Geometric Mean, namely,

$$\frac{a+b}{2} \geqslant \sqrt{ab}$$

Bogus proof

$$\begin{aligned} \frac{a+b}{2} &\geqslant \sqrt{ab} && \text{so} \\ a+b &\geqslant 2\sqrt{ab} && \text{so} \\ a^2+2ab+b^2 &\geqslant 4ab && \text{so} \\ a^2-2ab+b^2 &\geqslant 0 && \text{so} \\ (a-b)^2 &\geqslant 0 && \text{which we know is true.} \end{aligned}$$

So we have shown that $(a+b)/2 \geqslant \sqrt{ab}$. $\square$

What is wrong here and how can we fix it?

Take-away: NEVER start with what you want to prove.

Puzzle: The blue-eyed islanders

The islanders: 100 with blue eyes and 100 with brown eyes.

Puzzle: The blue-eyed islanders

The islanders: 100 with blue eyes and 100 with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

Puzzle: The blue-eyed islanders

The islanders: 100 with blue eyes and 100 with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in

Puzzle: The blue-eyed islanders

The islanders: 100 with blue eyes and 100 with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in
The guru: proclaims on Day 1 that someone on the island has blue eyes.

Puzzle: The blue-eyed islanders

The islanders: 100 with blue eyes and 100 with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in
The guru: proclaims on Day 1 that someone on the island has blue eyes.

The question: Who gets off the island and when?

Puzzle: The blue-eyed islanders

The islanders: **1** with blue eyes and **1** with brown eyes.

Puzzle: The blue-eyed islanders

The islanders: **1** with blue eyes and **1** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

Puzzle: The blue-eyed islanders

The islanders: **1** with blue eyes and **1** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in

Puzzle: The blue-eyed islanders

The islanders: **1** with blue eyes and **1** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in
The guru: proclaims on Day 1 that someone on the island has blue eyes.

Puzzle: The blue-eyed islanders

The islanders: **1** with blue eyes and **1** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in
The guru: proclaims on Day 1 that someone on the island has blue eyes.

The question: Who gets off the island and when?

Puzzle: The blue-eyed islanders

The islanders: **2** with blue eyes and **2** with brown eyes.

Puzzle: The blue-eyed islanders

The islanders: **2** with blue eyes and **2** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

Puzzle: The blue-eyed islanders

The islanders: 2 with blue eyes and **2** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in

Puzzle: The blue-eyed islanders

The islanders: **2** with blue eyes and **2** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in
The guru: proclaims on Day 1 that someone on the island has blue eyes.

Puzzle: The blue-eyed islanders

The islanders: **2** with blue eyes and **2** with brown eyes.

They don't know: their own eye color and they don't know the total number of blue-eyed people. Also they cannot talk to each other.

The pirate captain: visits every night and will free any *blue-eyed* person who can tell him their own eye color. (He will kill anyone who guesses incorrectly.) vspace.2in
The guru: proclaims on Day 1 that someone on the island has blue eyes.

The question: Who gets off the island and when?