Mathematical proofs

The application of logic in the demonstration of mathematical statements
On the nature of a mathematical proof

Mathematics is a “purely deductive” discipline. This means that mathematical statements are either axioms or theorems (i.e. lemmas, corollaries, propositions, theorems, etc)

– **Axioms** are statements declared to be true without proof

– **Theorems** are statements **derived** from true statements, using the rules of logic
Derivation

The “pattern of thinking” of the **derivation of a statement from previously known statements** is captured by the logical operation of **implication**.

Thus, the core of a **mathematical proof** is normally well represented as an **implication between predicates endowed with quantifiers** which we express symbolically as

\[ \Lambda(x, ..., z) H(x, ..., z) \Rightarrow \Omega(x, ..., z) T(x, ..., z) \]

- A combination of quantifiers
- The **hypothesis**: a true predicate
- A combination of quantifiers
- The **thesis**: Is it true or false?
Hidden implications

Quite often, mathematical statements do not show the implication explicitly. In most of these cases, the hypothesis appears to be missing.

– Example: Consider the classical trigonometric relation

\[ \sin^2 \theta + \cos^2 \theta = 1 \]

– The actual statement is

\[ (\forall \theta)(0 \leq \theta \leq 2\pi \implies \sin^2 \theta + \cos^2 \theta = 1) \]
Steps in reasoning about a proof

Before starting the proof:

• **Identify the actual logic structure of the theorem** (or given statement). **Rewrite** the theorem in terms of the identified logical structure.

• **Examine and decide on possible “proving strategies” and general style of the proof.** This depends on:
  – Previously proven statements and axioms that may have an influence in the proof; and
  – The logic and mathematical tools that are available to compose the proof
Main styles

• **Deductive proofs**
  – Direct proofs
  – Constructive proofs
  – Proofs by counterexample
  – Proofs by contrapositive
  – Proofs by reduction to absurdum

• **Inductive proofs**
  – Applies only to implications in which one of the predicate’s variable ranges over an infinite countable set
Proof by construction

- Applies to **existential** properties only

\[(\exists y)(\Lambda(x,\ldots, z)H(x,\ldots, y,\ldots, z) \Rightarrow \Omega(x,\ldots, z)T(x,\ldots, y,\ldots, z))\]

- Consist of two major steps:
  - Construction of a mathematical object
  - Proof that the constructed object satisfies the corresponding existential property
Example

**Theorem:** The set of all odd numbers is infinite countable

- **Rewrite as a logical statement:**

  If $\text{Odd} = \{n \in N : \exists m \in N \land n = 2m + 1\}$ then, there exists a function

  $f : N \to \text{Odd}$

  which is a bijection

- **Proving strategy:**

  By construction:
  - Build $f$
  - Demonstrate that the $f$ that has been built is a bijection
The demonstration

Proof: Let \( f(n)=2n+1 \), where \( n \) is a natural number. To show that \( f \) is a bijection:

- \( f \) is injective:
  
  Let \( p \neq q, p \in N \land q \in N \)
  
  Then, \( 2p + 1 \neq 2q + 1 \)
  
  Therefore, \( f(p) \neq f(q) \)

- \( f \) is onto:
  
  \((\forall m \in \text{Odd } )\exists n \in N \land m = 2n + 1\)
  
  \((\forall m \in \text{Odd } )\exists n \in N \land m = f(n)\)
Counterexamples

In practice one is often faced with the question: Is this statement true or false? Counterexamples are constructions used to demonstrate that a universal statement is false.

• A proof by counterexample is similar in spirit to a proof by construction and as such, it consists of the same two major steps:
  – Construction of a mathematical object
  – Demonstration that the constructed object makes the statement false
**Example**

*Theorem:* It is not the case that

\[(\forall x, y)(0 < x < y \Rightarrow x < y^2)\]

- **Rewrite as a logical statement:**
  Unnecessary

- **Proving strategy:**
  Counterexample. Find values for the variables that render the statement false.
Proof

Proof:

Let \( x = .5 \) and \( y = .6 \)

Then

\[
y^2 = .36 < .5 = x
\]
Direct proofs

By a **direct proof** it is normally understood a proof in which the implication is not replaced with its equivalent contrapositive form.

We distinguish two main cases:

- **Proof by exhaustion**
  - This is a proof in which all values of the predicate’s variables are verified with a direct **calculation**

- **Proof based on general arguments**
  - This is a proof in which general logical and/or mathematical arguments are used to demonstrate the implication
Example 1

**Theorem:**

\[(P \land Q) \Rightarrow (P \lor Q)\]

**Rewrite as logical statement:**
unnecessary

**Proving strategy:** By exhaustion

(it works!!: there are only four valuations)

**Proof:**

\[
\begin{array}{c|c|c|c|c|c}
P & Q & P \land Q & P \lor Q & () \Rightarrow () \\
0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
\end{array}
\]

Always true!
Example 2

**Theorem:** The product of two odd numbers is always an odd number

**Rewrite as a logical statement:**

\((\forall x, y)(x \in \text{Odd} \land y \in \text{Odd}) \Rightarrow xy \in \text{Odd}\)

**Proving strategy:** Direct. The rules of arithmetic will be used to show that the general form of an odd number is preserved under multiplication
Proof

**Proof:**
Let \( x \in \text{Odd} \land y \in \text{Odd} \)

Then, \((\exists n \in N)x = 2n + 1\) and \((\exists m \in N)y = 2m + 1\)

Now, \(xy = (2n + 1)(2m + 1)\)

\[
= (4nm + 2(n + m) + 1)
\]

\[
= 2(2nm + n + m) + 1
\]

Since \(k = 2nm + n + m \in N\)

\(xy = 2k + 1 \in \text{Odd}\)
Contrapositive forms

Replace the implication with its equivalent contrapositive form

– For a universal property:
  \((\forall y)(\neg T(x,\ldots, y,\ldots, z) \Rightarrow \neg H(x,\ldots, y,\ldots, z))\)

– For an existential property:
  \((\exists y)(\neg T(x,\ldots, y,\ldots, z) \Rightarrow \neg H(x,\ldots, y,\ldots, z))\)

Keep in mind that a contrapositive proof has nothing to do with the negation of the implication
Example

**Theorem:** If the square of a number is even, then so is the number.

**Rewrite in logical terms:**

Let $\text{Even} = \{x \in \mathbb{N} : (\exists n \in \mathbb{N}) x = 2n\}$

$(\forall x)(x^2 \in \text{Even} \Rightarrow x \in \text{Even})$

**Proving strategy:** A direct proof will involve the taking of a square root, which is not rich enough in arithmetic properties. The contrapositive replaces the square root with a multiplication.
Proof

Proof: The contrapositive is:

$(\forall x)(x \notin Even \Rightarrow x^2 \notin Even)$

Now, $x \notin Even \Rightarrow x \in Odd$

Therefore, $(\exists n \in N)x = 2n + 1$

But then, $x^2 = xx = (2n + 1)(2n + 1)$

$\hspace{2cm} = (4n^2 + 4n + 1)$

$\hspace{2cm} = 2(2n^2 + 2n) + 1$

Since $k = 2n^2 + 2n \in N$, $x^2 = 2k + 1 \in Odd$

Thus, $x^2 \notin Even$
Reduction to the absurdum

• It works by demonstrating that the \textit{negation of the implication} implies, in turn, a contradiction with an already accepted truth

• For proving $(H(x) \Rightarrow T(x))$ by contradiction
  – \textbf{Prove} $(H(x) \land \neg T(x)) \Rightarrow A(x)$
  – \textbf{Demonstrate that} $A(x)$ \textit{is false} (contradicts an established fact)
Example

**Theorem:** Let $U$ be an infinite set, $S$ be a finite subset of $U$, and $T$ the complement of $S$ with respect to $U$. Then, $T$ is infinite.

**Rewrite in logical terms:**

$$(\forall U)(U \text{ infinite}) \land (\forall S)(S \subseteq U \land \text{finite})$$

$T = U - S \Rightarrow T \text{ infinite}$

**Proving strategy:** Reduction to absurdum
Proof

Proof:
By contradiction: assume

\[ T = U - S \land \neg(T \text{ infinite}) \]

Then, \( T \) is finite

Since \( U = T \cup S \), \( U \) is the union of two finite sets

Contradiction:
The union of two finite sets is always a finite set

and \( U \) is infinite
Induction

• Recall that a set is **infinite countable** if it can be put in a one-to-one and onto correspondence with the set of natural numbers

• **Induction applies solely to predicates** of the form of

\[(\forall n)P(n)\]

where \( n \) ranges over a countable domain

• A **proof by induction** consists of two steps:
  – **Prove that** \((\exists n_0)P(n_0) = 1\)
  – **Prove that** \((\forall n \geq n_0)(P(n) \Rightarrow P(n + 1))\)
Example

**Theorem**: \( \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \)

Rewrite in logical terms:

\[
(\forall n)(n \in N \Rightarrow \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6})
\]

**Proving strategy**: Induction on \( n \)
Proof

Proof:

1. - Let $n_0 = 1$. Then, the statement becomes

$$\sum_{i=1}^{1} i^2 = \frac{1(2)(3)}{6} = 1$$

which is true.

2. - To show that:

$$(\forall n \geq 1)(\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}) \Rightarrow \sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

Proof : (next page)
Proof (continuation)

\[
\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2
\]

\[
= \frac{n(n+1)(2n+1)}{6} + (n^2 + 2n + 1)
\]

\[
= \frac{2n^3 + 3n^2 + n}{6} + \frac{6n^2 + 12n + 6}{6}
\]

\[
= \frac{2n^3 + 9n^2 + 13n + 6}{6}
\]

\[
= \frac{(n+1)(n+2)(2n+3)}{6}
\]