Video 13: Introduction to Proofs

- Theorems
- Mathematical Proofs
- Types of Proofs

Mathematicians develop Proofs

- Example of a mathematical genius
  - Many important contributions to number theory and analysis
  - When he was 15, a university student lent him a copy of Synopsis of Pure Mathematics. Ramanujan decided to work out the over 6000 results in this book, stated without proof or explanation, writing on sheets later collected to form notebooks

Srinivasa Ramanujanv
1887 - 1920

Proofs of Mathematical Statements

- A **mathematical proof** is a **valid argument** that establishes the truth of a statement
  - in particular of a theorem

Proofs of Mathematical Statements

- A **mathematical proof** is a **valid argument** that establishes the truth of a statement
  - in particular of a theorem
- A **theorem** is a statement that can be shown to be true using
  - definitions
  - axioms
  - other theorems
  - rules of inference

Proofs of Mathematical Statements

- A **mathematical proof** is a **valid argument** that establishes the truth of a statement
  - in particular of a theorem

- A **theorem** is a statement that can be shown to be true using
  - definitions
  - axioms
  - other theorems
  - rules of inference

- An **axiom** is a statement which is given as true

Informal Proofs

- In mathematics, computer science, and other disciplines, **informal proofs**, which are generally shorter, are often used

Informal Proofs

- In mathematics, computer science, and other disciplines, **informal proofs**, which are generally shorter, are often used
  - More than one rule of inference is used in a step
  - Steps may be skipped
  - The rules of inference used are not explicitly stated
  - Easier for to understand and to explain to people
  - **But it is also easier to introduce errors**

Applications of Proofs

- Apart from being at the core of mathematics, proofs have many practical applications as well
    - verification that computer programs are correct
    - establishing that operating systems are secure
    - enabling programs to make inferences in artificial intelligence
    - showing that system specifications are consistent

Terminology

- A **lemma** is a ‘helping theorem’ or a result which is needed to prove a theorem

Terminology

- A **lemma** is a ‘helping theorem’ or a result which is needed to prove a theorem
- A **corollary** is a result which follows directly from a theorem

Terminology

- A **lemma** is a ‘helping theorem’ or a result which is needed to prove a theorem
- A **corollary** is a result which follows directly from a theorem
- Less important theorems are sometimes called **propositions**

Terminology

- A **lemma** is a ‘helping theorem’ or a result which is needed to prove a theorem
- A **corollary** is a result which follows directly from a theorem
- Less important theorems are sometimes called **propositions**

- A **conjecture** is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.
  - Example: Fermat’s theorem has been a conjecture from 1634 - 1995

Forms of Theorems

Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or discrete structures

$$\forall x (P(x) \to Q(x))$$

Formulation of Theorems

Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

Formulation of Theorems

Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

“If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ ”

Formulation of Theorems

Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

“If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ ”

really means

“For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$.”

Proving Theorems

To prove theorems of the form $\forall x(P(x) \rightarrow Q(x))$

we show that $P(c) \rightarrow Q(c)$

where *c* is an arbitrary element of the domain.

Proving Theorems

To prove theorems of the form $\forall x(P(x) \to Q(x))$

we show that $P(c) \to Q(c)$

where *c* is an arbitrary element of the domain.

- By universal generalization the truth of the original formula follows.

Proving Theorems

To prove theorems of the form $\forall x(P(x) \to Q(x))$

we show that $P(c) \to Q(c)$

where *c* is an arbitrary element of the domain.

- By universal generalization the truth of the original formula follows.

- So, we must prove a statement of the form: $p \to q$

Proving Conditional Statements: $p \to q$

Proving Conditional Statements: $p \rightarrow q$

Trivial Proof: If we know q is true, then $p \rightarrow q$ is true as well.

Proving Conditional Statements: $p \to q$

Trivial Proof: If we know q is true, then $p \to q$ is true as well.

"If it is raining then 1 = 1."

Proving Conditional Statements: $p \to q$

Trivial Proof: If we know q is true, then $p \to q$ is true as well.

"If it is raining then 1 = 1."

Vacuous Proof: If we know p is false then $p \to q$ is true as well.

Proving Conditional Statements: $p \to q$

Trivial Proof: If we know q is true, then $p \to q$ is true as well.

"If it is raining then 1 = 1."

Vacuous Proof: If we know p is false then $p \to q$ is true as well.

"If I am both rich and poor then 2 + 2 = 5."

Direct Proofs for $p \rightarrow q$

Direct Proof: assume that p is true; then use definitions, axioms and theorems together with rules of inference till the statement q results

Indirect Proofs for $p \rightarrow q$

Proof by Contraposition: assume that $\neg q$ is True; then use definitions, axiom and theorems together with rules of inference till the statement $\neg p$ results

Indirect Proofs for $p \rightarrow q$

Proof by Contraposition: assume that $\neg q$ is True; then use definitions, axiom and theorems together with rules of inference till the statement $\neg p$ results

Since $p \rightarrow q \equiv \neg q \rightarrow \neg p$ the statement is proven

Indirect Proofs for $p \to q$

Proof by Contraposition: assume that $\neg q$ is True; then use definitions, axiom and theorems together with rules of inference till the statement $\neg p$ results

Since $p \to q \equiv \neg q \to \neg p$ the statement is proven

This is one type of an **indirect proof**

Indirect Proofs for $p \to q$

Proof by Contradiction: assume that p and $\neg q$ are true; then perform a direct proof to construct a contradiction, i.e., prove the statement ***F***

Indirect Proofs for $p \to q$

Proof by Contradiction: assume that p and $\neg q$ are true; then perform a direct proof to construct a contradiction, i.e., prove the statement $\boldsymbol{F}$

Since $p \to q \equiv (p \land \neg q) \to \boldsymbol{F}$ the statement is proven.

Indirect Proofs for $p \rightarrow q$

Proof by Contradiction: assume that p and $\neg q$ are true; then perform a direct proof to construct a contradiction, i.e., prove the statement $\boldsymbol{F}$

Since $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow \boldsymbol{F}$ the statement is proven.

AKA reductio ad absurdum, another type of indirect proof

Summary

- Axiom, Theorem, Proof
- Corollary, Lemma, Proposition, Conjecture
- Trivial and Vacuous Proof
- Direct Proof
- Indirect Proof: by contraposition and by contradiction