PROOF TECHNIQUES

A statement is either true or false.

- $1 = 0$ is ~~fal~~ false
- $\exists t : \cos(t) = t$ is true
- $\forall a, b, c, n : (n > 2) \wedge (a^n + b^n = c^n) \Rightarrow a = b = c = 0$
  is true

Some Statements may be true or false depending on the values assigned to variables

- $3x = 5$
- $x^2 + y^2 - 4xy > 0$

Definition: Proof

A mathematical proof is a convincing argument expressed in the language of mathematics

- the proof should be detailed enough to convince someone w/ reasonable background in the subject.

Terminology

Definition : an unambiguous explanation of terms

Proposition: a statement that is claimed to be true

Theorem : a major result

Lemma : a minor result; often used on the way to proving a ~~result~~ theorem

Corollary : something that follows from something just proved

Axioms : basic assumptions or truths

Forms of Theorems

A theorem can be reduced to stating "if A then B". The following are all equivalent:

- If A is true then B ~~B~~ is true
- $A \Rightarrow B$
- A implies B.
- A only if B
- A is sufficient for B
- B is true ~~t~~ whenever A is true

Proof Strategies

Forward-Backward Reasoning

- For any proof, you need a starting point.

Starting from the premises
- use axioms and theorems, construct a proof using a sequence of steps that leads to the conclusions.

This ~~is~~ type of reasoning is called forward reasoning.

Often forward reasoning is difficult if to prove complicated results because the reasoning needed to reach the conclusion is not obvious.

In such cases, using backward reasoning may be helpful.

Example

If a right angle triangle XYZ with sides of length x and y and a hypotenuse of length z has area $z^2/4$, then the triangle XYZ is isosceles.

"If A then B"

A: A right angle triangle XYZ with sides of length x and y and a hypotenuse of length z has area $z^2/4$

B: The triangle XYZ is isosceles

Backward reasoning
- How can I conclude B is true?
  - must be able to answer key questions
- Apply answer to specific problem
- Forward reason to this new point.

B: triangle XYZ is isosceles

How do I show B is true?

- How can I show a triangle is isosceles?
  - two sides are ~~to~~ equal
  - two angles are equal

- For our problem
  if we can show $x=y$ then we can show XYZ is isosceles.

- How do we show $x=y$?

- ~~When~~ How can I show ~~to~~ two real numbers are equal?
  - $x \le y \wedge y \le x$

    or
  - $x-y=0$ (B1)

Now from A if we can prove B1 then we can prove B

A $\quad \frac{1}{2}xy = \frac{z^2}{4}$ ① (area of triangle given)

$x^2+y^2 = z^2$ ② Pythagorean theorem

$\frac{1}{2}xy = \frac{x^2+y^2}{4}$ from ① & ②

$\Rightarrow x^2-2xy+y^2=0$ (algebra)

$\Rightarrow (x-y)^2=0$

$\Rightarrow x-y=0$

$\Rightarrow x=y \Rightarrow$ XYZ is isosceles

Notes

- Part of the proof is just algebraic manipulation
- other pieces drew on external information
  - def= of ~~isoo~~ isosceles triangle
  - eq= of area of triangle (theorem)
  - Pythagorean theorem
- In general, proofs will draw upon definition, axioms & previous proven theorems
- be careful to avoid a circular proof (i.e. a step in your proof relies on the theorem you are trying to prove.

Side
$q \Rightarrow r$
if q then r
(think of this as a promise)
Only time I break this promise is if q is T & r is F

Truth Table

$A \Rightarrow B$ "implies"

$\overline{B} \Rightarrow \overline{A}$ "contrapositive"

$B \Rightarrow A$ "converse"

$\overline{A} \Rightarrow \overline{B}$ "inverse"

$A \Leftrightarrow B$ "equivalence" "if & only if" "iff"

A	B	$\overline{A}$	$\overline{B}$	$A \Rightarrow B$	$\overline{B} \Rightarrow \overline{A}$	$B \Rightarrow A$	$\overline{A} \Rightarrow \overline{B}$	$A \Leftrightarrow B$
F	F	T	T	T	T	T	T	T
F	T	T	F	T	F	F	F	F
T	F	F	T	F	T	T	T	F
T	T	F	F	T	T	T	T	T

Quantifiers

- $\exists$: there exists an object w/ certain property such that something happens
- $\forall$: for all objects w/ a given properties

Specialization

- x' has a certain property
- $\forall x$ with a certain property, something happens
- the something happens for x'

Choose

- $\forall x$ with a certain property, something happens.
- Let x' be such that the certain property holds
- Something happens for x'

Examples

If s and t are rational & $t \neq 0$ then s/t is rational

step 1 A : s and t are rational

step 4 A1: $\exists\, x, y,\ y \neq 0 \ni s = p/q$

step 5 A2: Let a, b be such integers $\ni b \neq 0$ & $s = a/b$

step 6 A3: $\exists\, w, z,\ z \neq 0 \ni t = w/z$

step 7 A4: Let c, d be such integers $\ni d \neq 0$ & $t = c/d$

step 8 A5: $t \neq 0 \Rightarrow c \neq 0$

step 9 A6: $s/t = \dfrac{a/b}{c/d}$

$$= \frac{ad}{bc}$$

step 10 A7: Let $p = ad$ and $q = bc$

step 11 B2: $bc \neq 0$ $\quad \dfrac{s}{t} = \dfrac{ad}{bc} = \dfrac{p}{q}$

step 3 B1: $\exists\, p, q,\ q \neq 0 \ni s/t = p/q$

step 2 B : s/t is rational

If s and t are rational numbers and $t \neq 0$ the s/t is rational

Proof:

Let a, b be integers such that $s = a/b$ $(b \neq 0)$. Such integers must exist because ~~si~~ s is rational. Similarly, let c, d be integers such that $t = c/d$ $(d \neq 0)$. Since $t \neq 0$, it must be true that $c \neq 0$. Then, substituting $s/t = (a/b)/(c/d) = ad/bc$. $bc \neq 0$ since both b and c are non zero.

Therefore, s/t is rational because there exists p, q such that s/t is p/q.

Example

Proposition: If $f: X \to Y$ is onto and $g: Y \to Z$ is onto then $g \circ f: X \to Z$ is onto

Definitions: ① $f: S \to T$ is onto iff $\forall t \in T$, $\exists s \in S : f(s) = t$

(Surjection)

(range == codomain)

range: set of all images of ~~f(s)~~ elements of S

codomain: set T

② Let $f: X \to Y$ and $g: Y \to Z$ be function then $g \circ f: X \to Z$ is the function such that

$$(g \circ f)(x) = g(f(x))$$

$\underbrace{\text{If } f:X\to Y \text{ is onto and } g:Y\to Z \text{ is onto}}_{A}$, $\underbrace{\text{then } g\cdot f:X\to Z \text{ is onto}}_{B}$

1 A: $f:X\to Y$ is onto ~~&~~, $g:Y\to Z$ is onto

4 A1: ~~Let~~ Let $c\in Z$

6 A2: $\forall z\in Z \;\exists y\in Y \ni g(y)=z$

7 A3: $\exists y\in Y \ni g(y)=c$

8 A4: Let b be such a y: $b\in Y$, ~~g~~ $g(b)=c$

9 A5: $\forall y\in Y \;\exists x\in X \ni f(x)=y$

10 A6: $\exists x\in X \ni f(x)=b$

11 A7: Let a be such an x: $a\in X$, $f(a)=b$

12 A8: ~~Le~~ ~~g(b)=c~~ Let x of [B2] be a

14 A9: $(g\cdot f)(a)=g(f(a))=g(b)=c$

13 B3: $(g\cdot f)(a)=c$

5 B2: $\exists x\in X \ni (g\cdot f)(x)=c \quad \forall c\in Z$

3 B1 $\forall z\in Z, \exists x\in X \ni (g\cdot f)(x)=z$

2 B $g\cdot f: X\to Z$ is onto

If $f: X \to Y$ is onto and $g: Y \to Z$ is onto, then $g \cdot f : X \to Z$ is onto

Proof

for any $c \in Z$, we can find $b \in Y$ $\ni g(b) = c$ (Such b must exist $\because$ b is onto)

Similarly, let $a \in X$ be such that $f(a) = b$ (a must exist $\because$ f is onto). Then given any selected $c \in Z$, $(g \cdot f)(a) = c$ i.e. Some $a \in X$ can be found to make the claim true. $\therefore$ $g \cdot f : X \to Z$ is onto

PROOF BY CONTRADICTION

We assume that the negation of our proposition is true and show that it leads to a contradictory statement.

Example

Theorem: There are infinitely many prime numbers.

Proof: Suppose there is a finite numbers of primes numbers.
We can, therefore, list them in order:

$$p_1, p_2, \dots\ p_n$$

Consider the number q such that

$$q = p_1 p_2 \cdots p_n + 1$$

The number q can be either prime or composite

If we divide any of the listed primes p_i into q, there would be a remaider of 1.

Therefore, q cannot be composite.

Therefore, q is a prime not listed among the primes above, contradicting the assumption.

Example

Prove or disprove

If n^2 is even, then n is even

Proof by contradiction

Suppose n is odd, but n^2 is even

$n = 2k+1$

$$\begin{aligned} \therefore\ n^2 &= (2k+1)^2 \\ &= \underbrace{4k^2+4k}+1 \\ &= 2(2k^2+2k)+1 \\ &= 2j+1 \text{, which is odd} \end{aligned}$$

This contradicts our assumption.

PROOF BY INDUCTION

Three steps

- Start by verifying the base case
- Then assume the n^{th} case ~~is~~ holds
- Use that to prove the $(n+1)^{st}$ case

Strong Induction

- Start by verifying the base case
- Then assume the statement holds for all ~~case~~ values preceding and equal to n.
- Use that to prove the $(n+1)^{st}$ case holds

Example

Prove $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ for $n \geq 0$

- Base case $n = 0$

$$\sum_{i=0}^{0} i = 0 = \frac{0.(0+1)}{2}$$

$$0 = 0$$

True $\therefore$ The base case holds

- Inductive step

Assume $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

for $n+1$

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$

By transitivity of equality $\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}$

Example

Prove that the sum of the first n odd positive integers is n^2

Base case

The first odd positive integer is 1.

$\therefore$ the sum of the first positive integer is

$1 = 1^2$

$\therefore$ The base case is true

Inductive Hypothesis

Assume $1 + 3 + 5 + \ldots + (2n-1) = n^2$

we must show $1+3+5+\ldots + (2n-1) + (2n+1) = (n+1)^2$

$1+3+5+\ldots + (2n-1) + (2n+1)$

$=$ <Inductive Hypothesis>

$n^2 + (2n+1)$

$=$

(n^2+2n+1)

<algebra>

$= (n+1)^2$

$\therefore$ by transitivity of equality

$1+3+5+\ldots + (2n-1) + (2n+1) = (n+1)^2$

$\therefore$ By mathematical induction the sum of the first n odd positive integers is n^2

Example

Prove that if S is a finite set with n elements, the S has 2^n subsets $(n \geq 0)$

Base case: $(n=0)$

a set S of size 0 has one subset (the empty set); $2^0 = 1$

$\therefore$ the base case is true

Inductive Step

Assume that every set w/ n elements has 2^n subsets.

Let S be a set w/ n elements $\therefore$ it has 2^n subsets

Let T be a set ~~w/ n+1 elements~~ by adding 1 element to S

$\therefore T$ has $n+1$ elements

$T = S \cup \{a\}$.

For each subset x of S, there are exactly two subsets of T, x & $x \cup \{a\}$.

There are 2^n subsets of S.

There fore there are 2×2^n subsets of T

$2 \times 2^n = 2^{n+1}$