Introduction to Proofs

CSC165 Week 3 - Part 1

Lindsey Shorser, Winter 2021

$$x^2 + y^2 \geq 2xy$$

$$x^2 - 2xy + y^2 \geq 0$$

$$(x - y)^2 \geq 0$$

$$(x - y)^2 \geq 0$$

$$x^2 - 2xy + y^2 \geq 0$$

$$x^2 + y^2 \geq 2xy$$

Prove that for all x, y in $\mathbb{R}$,

$$x^2 + y^2 \geq 2xy.$$

$$x^2 + y^2 \geq 2xy$$

$$x^2 - 2xy + y^2 \geq 0$$

$$(x - y)^2 \geq 0$$

$$(x - y)^2 \geq 0$$

$$x^2 - 2xy + y^2 \geq 0$$

$$x^2 + y^2 \geq 2xy$$

Claim: $\forall x, y \in \mathbb{R},\ x^2 + y^2 \geq 2xy.$

Proof: Fix x in $\mathbb{R}$ and y in $\mathbb{R}$.

$(x - y)^2 \geq 0$

$x^2 - 2xy + y^2 \geq 0$

$x^2 + y^2 \geq 2xy$

Since x and y could be any real number, we can conclude that

$$\forall x, y \in \mathbb{R},\ x^2 + y^2 \geq 2xy.$$

What are we proving?

- Does it have quantifiers? If so, which one(s)?
- What are the logical operations?
- Is the statement true or false?

$\forall\ s \in S$

$\exists\ s \in S$

Arbitrary Elements

These are elements of a set that could be any element.

An arbitrary even integer: $x = 2k$ for some $k \in \mathbb{Z}$

An arbitrary odd integer: $x = 2k + 1$ for some $k \in \mathbb{Z}$

An arbitrary polynomial: $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$

where $a_i \in \mathbb{R}$, $i = 0, 1, \dots n$ for some $n \in \mathbb{N}$

An arbitrary degree 2 polynomial: $p(x) = a_2 x^2 + a_1 x + a_0$

where $a_i \in \mathbb{R}$, $i = 0, 1, 2$

Example:

Prove or disprove that all primes are Mersenne primes.

The definition of n being a Mersenne prime is:

The natural number n is a Mersenne Prime if and only if it can be written as $2^k - 1$ for some positive integer k.

In symbols, this looks like:

We want to show that not all primes are Mersenne primes.

in symbols this looks like:

Rough work:

Proof:

What goes into a proof:

- The header
  - what we want to show,
  - “let” statements,
  - any assumptions we can make
- The body of the proof is an argument that relies on:
  - definitions
  - assumptions that were made in the proof header
  - previous deductions from something that already appeared in the proof body
  - external true statements that we already know

Prove or disprove:

$$\forall\, n \in \mathbb{N},\ n > 20 \Rightarrow 1.5n - 4 \geq 3$$

$$\forall\, n \in \mathbb{N},\ n > 20 \wedge 1.5n - 4 \geq 3$$

$$\exists\, n \in \mathbb{N},\ n > 20 \wedge 1.5n - 4 \geq 3$$

$$\exists\, n \in \mathbb{N},\ n > 20 \Rightarrow 1.5n - 4 \geq 3$$

A typical proof of an existential.

Given statement to prove: $\exists x \in S,\ P(x)$.

Proof. Let $x =$ ________.

[Proof that $P($________$)$ is True.]

$\blacksquare$

A typical proof of a universal.

Given statement to prove: $\forall x \in S, P(x)$.

Proof. Let $x \in S$. (That is, let x be an arbitrary element of S.)

[Proof that $P(x)$ is True].

$\blacksquare$

A typical proof of an implication (direct).

Given statement to prove: $p \Rightarrow q$.

Proof. Assume p.

[Proof that q is True.]

$\blacksquare$

Prove or disprove:

$$\forall\, n \in \mathbb{N},\ n > 20 \Rightarrow 1.5n - 4 \geq 3$$

$$\forall\, n \in \mathbb{N},\ n > 20 \wedge 1.5n - 4 \geq 3$$

$$\exists\, n \in \mathbb{N},\ n > 20 \wedge 1.5n - 4 \geq 3$$

$$\exists\, n \in \mathbb{N},\ n > 20 \Rightarrow 1.5n - 4 \geq 3$$

Example: $\forall x \in \mathbb{Z}, \; x \mid x + 5 \Rightarrow x \mid 5.$

Proof: