Introduction to Proofs

CSC165 Week 3 - Part 1

Lindsey Shorser, Winter 2021

Rough Work

by arithmetic:

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

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

by factoring:

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

The body of a proof:
(looks like an argument)

We know:

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

by property of exponents

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

by arithmetic

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

by arithmetic

$\forall x \in \mathbb{R}, \forall y \in \mathbb{R}$

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

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

Rough Work

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

$\Updownarrow$

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

$\Updownarrow$

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

$\downarrow$

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

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

$\downarrow$

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

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

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

Let $x \in \mathbb{R}$ and $y \in \mathbb{R}$.

We already know that squares are positive or zero, so:

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

$$\Rightarrow \quad x^2 - 2xy + y^2 \geq 0 \quad \text{by arithmetic}$$

$$\Rightarrow \quad x^2 + y^2 \geq 2xy \quad \text{by arithmetic}$$

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?

$\wedge \vee \Rightarrow$ etc.

$\forall\ s \in S$ Fix s.

(choose an arbitrary element so that we don't know anything about it other than it is in S)

$\exists\ s \in S$ Find s, show that

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

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

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

where $a_i \in \mathbb{R}$, $i = 0, 1, 2$, $a_2 \neq 0$

$ax^2 + bx + c \quad a \neq 0$

Example:

all A_s are B_s

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. and is prime.

In symbols, this looks like:

Let Prime(n) = "n is prime", M(n) = "n is a Mersenne prime".

$$\neg(\forall n \in \mathbb{N},\ Prime(n) \Rightarrow M(n))$$

$$\exists n \in \mathbb{N},\ Prime(n) \wedge \neg M(n)$$

$\neg(P \Rightarrow M)$

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

Header: in symbols this looks like:

We want to show that:

$$\exists n \in \mathbb{N}, \text{Prime}(n) \wedge \neg(\exists k \in \mathbb{Z}^+, n = 2^k - 1)$$

Let Prime(n) = "n is a prime number" where prime means "has exactly two distinct factors,1 and itself." Also, let M(n) = "n is a Mersenne prime", where Mersenne prime means there is a pos. integer k such that $n = 2^k - 1$

Rough work:

$k = 1, \quad 2^1 - 1 \quad \times$

$k = 2, \quad 2^2 - 1 = 3$

$k = 3, \quad 2^3 - 1 = 7$

$5?$ $\quad 2^k - 1 \neq 5$

Proof:

Let n = 5.

n is prime because its factors are 1 and 5.

If there is a positive integer k such that

$$5 = 2^k - 1$$

$$\Rightarrow 6 = 2^k$$

$$\Rightarrow \log_2 6 = k \notin \mathbb{Z}^+$$

$$\therefore \exists n \in \mathbb{N}, \text{ Prime}(n) \wedge \neg M(n)$$

Q.E.D

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:

$y = 1.5x - 4$ is an increasing line

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

Let n be a natural number and assume that $n > 20$.

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

Find a counterexample that shows there exists n that is not > 20.

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

Find n that is > 20 and such that 1.5n - 4 is greater than or equal to 3.

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

Find an n such that if n>20 then ...

A typical proof of an existential.

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

Proof. Let $x =$ __5__.

[Proof that $P($__5__$)$ is True.]

■

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].

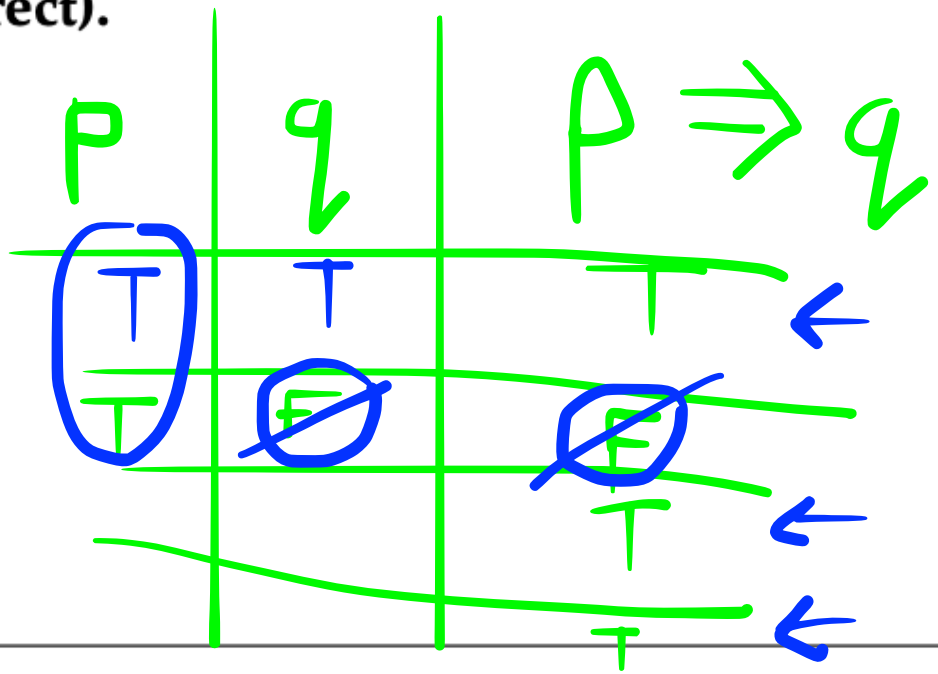
■

A typical proof of an implication (direct).

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

Proof. Assume p.

[Proof that q is True.]



■

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: