Proofs and Analysis

James Wright[1]

September 23, 2011

[1] Based on (almost identical to) Matt Hoffman's 2009 refresher.

Overview

1. Two lightning-fast notation slides.
2. Proof techniques, with some straightforward examples.
3. Basic definitions from analysis.
4. Example proofs.

Logic

Notation:

$\neg A$	not A
$A \vee B$	A or B
$A \wedge B$	A and B
$A \Rightarrow B$	A implies B
$A \iff B$	A if and only if B

A	B	$A \Rightarrow B$
False	False	True
False	True	True
True	False	False
True	True	True

Logical equivalences:

- $A \Rightarrow B \equiv \neg A \vee B$
- $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

Notation:

$x \in A$	x is an element of A.
$\{x \in A \mid P(x)\}$	Set of elements of A satisfying predicate P.
$\overline{A}$	Complement of A: $\{x \mid x \notin A\}$
$A \cup B$	Union of A and B: $\{x \mid (x \in A) \vee (x \in B)\}$.
$A \cap B$	Intersection of A and B: $\{x \mid (x \in A) \wedge (x \in B)\}$.
$A \backslash B$	Set difference: $\{x \in A \mid x \notin B\}$.
$A \times B$	Cross product: $\{(x, y) \mid (x \in A) \wedge (y \in B)\}$.
$\mathcal{P}(A)$	Power set: $\{B \mid B \subseteq A\}$.
$\lvert A \rvert$	Cardinality; number of elements of A.[2]

[2] For finite A.

Direct proof

- Most theorems can be stated as an implication:
  1. The sum of two rational numbers is rational.

     $$a, b \in Q \Rightarrow a + b \in Q$$

  2. Every odd integer is the difference of two perfect squares:

     $$i = 2j + 1 \text{ for } j \in \mathbb{Z} \Rightarrow \exists a, b \in \mathbb{N} : i = a^2 - b^2$$

- If we assume that the LHS is true and can then show the RHS is true, then the implication must be true.

Direct proof

- Most theorems can be stated as an implication:
  1. The sum of two rational numbers is rational.

     $$a, b \in Q \Rightarrow a + b \in Q$$

  2. Every odd integer is the difference of two perfect squares:

     $$i = 2j + 1 \text{ for } j \in \mathbb{Z} \Rightarrow \exists a, b \in \mathbb{N} : i = a^2 - b^2$$

- If we assume that the LHS is true and can then show the RHS is true, then the implication must be true.

Proof.

Assume that $i = 2j + 1$. We can write that as

$$i = 2j + 1$$

Direct proof

- Most theorems can be stated as an implication:
  1. The sum of two rational numbers is rational.

     $$a, b \in Q \Rightarrow a + b \in Q$$

  2. Every odd integer is the difference of two perfect squares:

     $$i = 2j + 1 \text{ for } j \in \mathbb{Z} \Rightarrow \exists a, b \in \mathbb{N} : i = a^2 - b^2$$

- If we assume that the LHS is true and can then show the RHS is true, then the implication must be true.

Proof.
Assume that $i = 2j + 1$. We can write that as

$$\begin{aligned} i &= 2j + 1 \\ &= j^2 - j^2 + 2j + 1 \end{aligned}$$

Direct proof

- Most theorems can be stated as an implication:
  1. The sum of two rational numbers is rational.
  $$a, b \in Q \Rightarrow a + b \in Q$$
  2. Every odd integer is the difference of two perfect squares:
  $$i = 2j + 1 \text{ for } j \in \mathbb{Z} \Rightarrow \exists a, b \in \mathbb{N} : i = a^2 - b^2$$
- If we assume that the LHS is true and can then show the RHS is true, then the implication must be true.

Proof.
Assume that $i = 2j + 1$. We can write that as

$$\begin{aligned} i &= 2j + 1 \\ &= j^2 - j^2 + 2j + 1 \\ &= (j + 1)^2 - j^2. \end{aligned}$$

□

Proof by contrapositive

Like a direct proof, but we first use the equivalence
$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$.
So, assume the RHS is false, and then show that the LHS is also.

Example

Show that if $3n + 2$ is even then n is even.

Proof by contrapositive

Like a direct proof, but we first use the equivalence
$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$.
So, assume the RHS is false, and then show that the LHS is also.

Example

Show that if $3n + 2$ is even then n is even.

Instead we will show that if n is not even, then $3n + 2$ is not even.
I.e., if n is odd then $3n + 2$ is odd.

Proof by contrapositive

Like a direct proof, but we first use the equivalence
$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$.
So, assume the RHS is false, and then show that the LHS is also.

Example

Show that if $3n + 2$ is even then n is even.

Instead we will show that if n is not even, then $3n + 2$ is not even.
I.e., if n is odd then $3n + 2$ is odd.

Proof.

Assume that n is odd. That is, $n = 2j + 1$ for some $j \in \mathbb{N}$.

$$3n + 2 = 3(2j + 1) + 2$$

Proof by contrapositive

Like a direct proof, but we first use the equivalence
$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$.
So, assume the RHS is false, and then show that the LHS is also.

Example

Show that if $3n + 2$ is even then n is even.

Instead we will show that if n is not even, then $3n + 2$ is not even.
I.e., if n is odd then $3n + 2$ is odd.

Proof.

Assume that n is odd. That is, $n = 2j + 1$ for some $j \in \mathbb{N}$.

$$\begin{aligned} 3n + 2 &= 3(2j + 1) + 2 \\ &= 6j + 5 \end{aligned}$$

Proof by contrapositive

Like a direct proof, but we first use the equivalence
$A \Rightarrow B \equiv \neg B \Rightarrow \neg A$.
So, assume the RHS is false, and then show that the LHS is also.

Example

Show that if $3n + 2$ is even then n is even.

Instead we will show that if n is not even, then $3n + 2$ is not even.
I.e., if n is odd then $3n + 2$ is odd.

Proof.

Assume that n is odd. That is, $n = 2j + 1$ for some $j \in \mathbb{N}$.

$$\begin{aligned} 3n + 2 &= 3(2j + 1) + 2 \\ &= 6j + 5 \\ &= 2(3j + 2) + 1, \end{aligned}$$

hence $3n + 2$ is odd. □

Proof by induction

We want to prove an infinite number of statements $A_0, A_1, A_2, \ldots$.

- Prove that $A_n \Rightarrow A_{n+1}$ for any n (the inductive case).
- Prove A_0 (the base case).

Proof by induction

We want to prove an infinite number of statements $A_0, A_1, A_2, \ldots$.

- Prove that $A_n \Rightarrow A_{n+1}$ for any n (the inductive case).
- Prove A_0 (the base case).
- Like dominoes, $A_0 \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \ldots$.

Proof by induction

Example

Prove that the number of subsets of a set with n elements is 2^n.

Example

Prove that the number of subsets of a set with n elements is 2^n.

Proof.

Base case: The set with 0 elements, $\varnothing$ has exactly $2^0 = 1$ subset.

Proof by induction

Example

Prove that the number of subsets of a set with n elements is 2^n.

Proof.

Base case: The set with 0 elements, $\varnothing$ has exactly $2^0 = 1$ subset.
Inductive case: Assume that all sets of size k have 2^k subsets.
Choose an arbitrary set B of size $k + 1$.
Choose an element $x \in B$ and let $A = B \backslash \{x\}$. So $B = A \cup \{x\}$.

Example

Prove that the number of subsets of a set with n elements is 2^n.

Proof.

Base case: The set with 0 elements, $\varnothing$ has exactly $2^0 = 1$ subset.
Inductive case: Assume that all sets of size k have 2^k subsets.
Choose an arbitrary set B of size $k+1$.
Choose an element $x \in B$ and let $A = B \backslash \{x\}$. So $B = A \cup \{x\}$.
$\mathcal{P}(B) = \mathcal{P}(A) \cup \{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}$, so we have:

Proof by induction

Example

Prove that the number of subsets of a set with n elements is 2^n.

Proof.

Base case: The set with 0 elements, $\varnothing$ has exactly $2^0 = 1$ subset.
Inductive case: Assume that all sets of size k have 2^k subsets.
Choose an arbitrary set B of size $k + 1$.
Choose an element $x \in B$ and let $A = B \backslash \{x\}$. So $B = A \cup \{x\}$.
$\mathcal{P}(B) = \mathcal{P}(A) \cup \{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}$, so we have:

$$|\mathcal{P}(B)| = |\mathcal{P}(A)| + |\{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}|$$

because $\mathcal{P}(A)$ and $\{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}$ are disjoint

Example

Prove that the number of subsets of a set with n elements is 2^n.

Proof.

Base case: The set with 0 elements, $\varnothing$ has exactly $2^0 = 1$ subset.
Inductive case: Assume that all sets of size k have 2^k subsets.
Choose an arbitrary set B of size $k+1$.
Choose an element $x \in B$ and let $A = B \backslash \{x\}$. So $B = A \cup \{x\}$.
$\mathcal{P}(B) = \mathcal{P}(A) \cup \{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}$, so we have:

$$\begin{aligned} |\mathcal{P}(B)| &= |\mathcal{P}(A)| + |\{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}| \\ &= |\mathcal{P}(A)| + |\mathcal{P}(A)| \end{aligned}$$

Proof by induction

Example

Prove that the number of subsets of a set with n elements is 2^n.

Proof.

Base case: The set with 0 elements, $\varnothing$ has exactly $2^0 = 1$ subset.
Inductive case: Assume that all sets of size k have 2^k subsets.
Choose an arbitrary set B of size $k+1$.
Choose an element $x \in B$ and let $A = B \backslash \{x\}$. So $B = A \cup \{x\}$.
$\mathcal{P}(B) = \mathcal{P}(A) \cup \{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}$, so we have:

$$\begin{aligned} |\mathcal{P}(B)| &= |\mathcal{P}(A)| + |\{A' \cup \{x\} \mid A' \in \mathcal{P}(A)\}| \\ &= |\mathcal{P}(A)| + |\mathcal{P}(A)| \\ &= 2|\mathcal{P}(A)| \\ &= 2 \cdot 2^k \text{ (by induction)} \\ &= 2^{k+1}. \end{aligned}$$

□

General induction

We want to prove an infinite number of statements $A_0, A_1, A_2, \ldots$

- Prove that $A_0 \wedge A_1 \wedge \ldots \wedge A_n \Rightarrow A_{n+1}$ for any n (the inductive case).
- Prove A_0 (the base case).

General induction

We want to prove an infinite number of statements $A_0, A_1, A_2, \ldots$

- Prove that $A_0 \wedge A_1 \wedge \ldots \wedge A_n \Rightarrow A_{n+1}$ for any n (the inductive case).
- Prove A_0 (the base case).
- Like dominoes,

$$
\begin{aligned}
A_0 &\Rightarrow A_1 \\
A_0 \wedge A_1 &\Rightarrow A_2 \\
A_0 \wedge A_1 \wedge A_2 &\Rightarrow A_3 \\
&\ldots
\end{aligned}
$$

Example

Prove that for any $n \in \mathbb{N}$, $n = p_1 p_2 \dots p_k$,
where p_i is prime for all $1 \leq i \leq k$.

Example

Prove that for any $n \in \mathbb{N}$, $n = p_1 p_2 \ldots p_k$,
where p_i is prime for all $1 \leq i \leq k$.

Proof.

Base case: $n = 2, k = 1, p_1 = 2$.

Example

Prove that for any $n \in \mathbb{N}$, $n = p_1 p_2 \dots p_k$,
where p_i is prime for all $1 \leq i \leq k$.

Proof.

Base case: $n = 2, k = 1, p_1 = 2$.
Inductive case: Assume $w = p_1 p_2 \dots p_k$ for all $w < n$.
Case 1: n is prime. Then $p_1 = n$ and we're done.

Example

Prove that for any $n \in \mathbb{N}$, $n = p_1 p_2 \ldots p_k$,
where p_i is prime for all $1 \leq i \leq k$.

Proof.

Base case: $n = 2, k = 1, p_1 = 2$.
Inductive case: Assume $w = p_1 p_2 \ldots p_k$ for all $w < n$.
Case 1: n is prime. Then $p_1 = n$ and we're done.
Case 2: n is composite. So $n = ab$ for $a, b \in \mathbb{N}$ and $a, b > 1$.

Example

Prove that for any $n \in \mathbb{N}$, $n = p_1 p_2 \ldots p_k$,
where p_i is prime for all $1 \leq i \leq k$.

Proof.

Base case: $n = 2, k = 1, p_1 = 2$.
Inductive case: Assume $w = p_1 p_2 \ldots p_k$ for all $w < n$.
Case 1: n is prime. Then $p_1 = n$ and we're done.
Case 2: n is composite. So $n = ab$ for $a, b \in \mathbb{N}$ and $a, b > 1$.
By induction, $a = p_1 p_2 \ldots p_k$ and $b = p'_1 p'_2 \ldots p'_{k'}$.
Hence $n = p_1 p_2 \ldots p_k p'_1 p'_2 \ldots p'_{k'}$. □

Proof by contradiction

We want to prove some statement A.
Instead, we assume $\neg A$ and show that it leads to some contradiction.
Everything was consistent without $\neg A$, so it must have been $\neg A$ that caused the inconsistency/contradiction.
Therefore, $\neg\neg A \equiv A$ must be true.

Proof by contradiction

We want to prove some statement A.
Instead, we assume $\neg A$ and show that it leads to some contradiction.
Everything was consistent without $\neg A$, so it must have been $\neg A$ that caused the inconsistency/contradiction.
Therefore, $\neg\neg A \equiv A$ must be true.

Example

Prove that $ab + 1 \neq ac$ for any $a, b, c \in \mathbb{N}$ where $a, b, c > 1$.

Proof by contradiction

We want to prove some statement A.
Instead, we assume $\neg A$ and show that it leads to some contradiction.
Everything was consistent without $\neg A$, so it must have been $\neg A$ that caused the inconsistency/contradiction.
Therefore, $\neg\neg A \equiv A$ must be true.

Example

Prove that $ab + 1 \neq ac$ for any $a, b, c \in \mathbb{N}$ where $a, b, c > 1$.

Proof.

Assume instead that $ac = ab + 1$.
Then by rearrangement we have $c = b + \frac{1}{a}$.
But since $a > 1$, $b + \frac{1}{a} \notin \mathbb{N}$, a contradiction. □

Infimum and supremum

Consider a set T ordered by relation $\leq$ and a subset $S \subseteq T$.

- The infimum is the greatest lower bound.
- The supremum is the least upper bound.

These bounds are the tightest possible on S, but they need not be in S.

- Hence they differ from min and max.
- For $T \neq \mathbb{R}$, they need not even exist.

Infimum and supremum

Consider a set T ordered by relation $\leq$ and a subset $S \subseteq T$.

- The infimum is the greatest lower bound.
- The supremum is the least upper bound.

These bounds are the tightest possible on S, but they need not be in S.

- Hence they differ from min and max.
- For $T \neq \mathbb{R}$, they need not even exist.

Example

Let $T = \mathbb{R}$ and $S = \{x \in \mathbb{R} \mid x^2 < 2\}$.
Then $\sup(S) = \sqrt{2}$, but $\sqrt{2} \notin S$.
So $\max(S)$ does not exist.

Miscellaneous notation: arg min and arg max

Definition

The arg min of an expression $f(x)$ is the set of values of x for which the expression attains its minimum. That is,

$$\arg\min_{x \in X} f(x) = \{x \in X \mid f(x) \geq f(x') \quad \forall x' \in X\}.$$

The arg max is defined analogously for the maximum.

Example

$$\arg\min_{x \in \mathbb{R}} x^2 + 5 = \{0\}.$$

$$\arg\min_{x \in \{-2,5,2\}} \log|x| = \{-2, 2\}.$$

$$\arg\min_{x \in \mathbb{R}} \log|x| \text{ does not exist.}$$

Definition

A function has a limit

$$\lim_{x \to x_0} f(x) = L$$

if for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$|f(x) - L| < \epsilon \text{ if } |x - x_0| < \delta.$$

Definition

For limits tending to infinity,

$$\lim_{x \to \infty} f(x) = L$$

if for every $\epsilon > 0$ there exists a bound $M > 0$ such that

$$|f(x) - L| < \epsilon \text{ if } x > M.$$

Example

Show that $\lim_{x\to\infty} \frac{2x-1}{x-3} = 2$.

Proof.

Using the definition, we can write

$$\begin{aligned} |f(x) - L| &= \frac{2x-1}{x-3} - 2 \\ &= \frac{2x-1}{x-3} - \frac{2x-6}{x-3} \\ &= \frac{5}{x-3}. \end{aligned}$$

We can see that if $x > 3 + \frac{5}{\epsilon} \Rightarrow |f(x) - L| < \epsilon$ (provided that $x > 3$). □

Definition

$f(x)$ is continuous at x_0 if $\lim_{x \to x_0} f(x) = f(x_0)$. $f(x)$ is continuous on $[a, b]$ if this holds for all $x_0 \in [a, b]$.

Theorem (Intermediate value theorem)

If $f(x)$ is continuous on $[a, b]$, then f takes on every value between $f(a)$ and $f(b)$.

Cardinality of $\mathbb{R}$

Theorem

The real numbers are uncountable. That is, no enumeration exists that assigns to every element of $\mathbb{R}$ a unique element of $\mathbb{N}$.

Cardinality of $\mathbb{R}$

Theorem

The real numbers are uncountable. That is, no enumeration exists that assigns to every element of $\mathbb{R}$ a unique element of $\mathbb{N}$.

Proof (by contradiction).

Assume, on the contrary, that $[0, 1]$ is countable, and thus we can construct an infinite list containing all the reals in this range:

0	0.0
1	$0.14159\ldots$
2	$0.7182817\ldots$
$\vdots$	

Cardinality of $\mathbb{R}$

Theorem

The real numbers are uncountable. That is, no enumeration exists that assigns to every element of $\mathbb{R}$ *a unique element of* $\mathbb{N}$*.*

Proof (by contradiction).

Assume, on the contrary, that $[0, 1]$ is countable, and thus we can construct an infinite list containing all the reals in this range:

0	0.0
1	$0.14159\ldots$
2	$0.7182817\ldots$
$\vdots$	

Let k_n be the nth digit of the nth number.

Now construct w whose nth digit is 2 if $k_n = 1$, or 1 otherwise.

Theorem

The real numbers are uncountable. That is, no enumeration exists that assigns to every element of $\mathbb{R}$ a unique element of $\mathbb{N}$.

Proof (by contradiction).

Assume, on the contrary, that $[0, 1]$ is countable, and thus we can construct an infinite list containing all the reals in this range:

0	0.0
1	0.14159...
2	0.7182817...
⋮	

Let k_n be the nth digit of the nth number.

Now construct w whose nth digit is 2 if $k_n = 1$, or 1 otherwise. Note that w cannot appear on our list, because it differs from the nth number in the list in the nth digit. Therefore the list does not contain all the reals in $[0, 1]$ after all, a contradiction. □

Cardinality of $\mathbb{Q}$

Guesses about the cardinality of $\mathbb{Q}$?

Example

The rational numbers are countable: There exists an enumeration that assigns to every element of $\mathbb{Q}$ a unique element of $\mathbb{N}$.

Proof (direct by construction).

We demonstrate that the rationals are countable by constructing an enumeration. Create a table with numerators across the top and denominators down the sides:

$\mathbb{Q}$	1	2	3...
1	1/1	2/1	3/1...
2	1/2	2/2	3/2...
3	1/3	2/3	3/3...
⋮			

Start at the top-left and zig-zag across the table, counting fully-reduced fractions as you go:

{ }.

Example

The rational numbers are countable: There exists an enumeration that assigns to every element of $\mathbb{Q}$ a unique element of $\mathbb{N}$.

Proof (direct by construction).

We demonstrate that the rationals are countable by constructing an enumeration. Create a table with numerators across the top and denominators down the sides:

$\mathbb{Q}$	1	2	3...
1	1/1	2/1	3/1...
2	1/2	2/2	3/2...
3	1/3	2/3	3/3...
$\vdots$			

Start at the top-left and zig-zag across the table, counting fully-reduced fractions as you go:

$\{(1, \frac{1}{1}),$ $\}.$

Example

The rational numbers are countable: There exists an enumeration that assigns to every element of $\mathbb{Q}$ a unique element of $\mathbb{N}$.

Proof (direct by construction).

We demonstrate that the rationals are countable by constructing an enumeration. Create a table with numerators across the top and denominators down the sides:

$\mathbb{Q}$	1	2	3...
1	1/1	2/1	3/1...
2	1/2	2/2	3/2...
3	1/3	2/3	3/3...
$\vdots$			

Start at the top-left and zig-zag across the table, counting fully-reduced fractions as you go:

$\{(1, \frac{1}{1}), (2, \frac{2}{1}), \qquad \}.$

Example

The rational numbers are countable: There exists an enumeration that assigns to every element of $\mathbb{Q}$ a unique element of $\mathbb{N}$.

Proof (direct by construction).

We demonstrate that the rationals are countable by constructing an enumeration. Create a table with numerators across the top and denominators down the sides:

$\mathbb{Q}$	1	2	3...
1	1/1	2/1	3/1...
2	1/2	2/2	3/2...
3	1/3	2/3	3/3...
⋮			

Start at the top-left and zig-zag across the table, counting fully-reduced fractions as you go:
$\{(1, \frac{1}{1}), (2, \frac{2}{1}), (3, \frac{1}{2}), \qquad \}$.

Cardinality of $\mathbb{Q}$

Example

The rational numbers are countable: There exists an enumeration that assigns to every element of $\mathbb{Q}$ a unique element of $\mathbb{N}$.

Proof (direct by construction).

We demonstrate that the rationals are countable by constructing an enumeration. Create a table with numerators across the top and denominators down the sides:

$\mathbb{Q}$	1	2	3...
1	1/1	2/1	3/1...
2	1/2	2/2	3/2...
3	1/3	2/3	3/3...
⋮			

Start at the top-left and zig-zag across the table, counting fully-reduced fractions as you go:
$\{(1, \frac{1}{1}), (2, \frac{2}{1}), (3, \frac{1}{2}), (4, \frac{3}{2}), \quad \}$.

Cardinality of $\mathbb{Q}$

Example

The rational numbers are countable: There exists an enumeration that assigns to every element of $\mathbb{Q}$ a unique element of $\mathbb{N}$.

Proof (direct by construction).

We demonstrate that the rationals are countable by constructing an enumeration. Create a table with numerators across the top and denominators down the sides:

$\mathbb{Q}$	1	2	3...
1	1/1	2/1	3/1...
2	1/2	2/2	3/2...
3	1/3	2/3	3/3...
⋮			

Start at the top-left and zig-zag across the table, counting fully-reduced fractions as you go:
$\{(1, \frac{1}{1}), (2, \frac{2}{1}), (3, \frac{1}{2}), (4, \frac{3}{2}), (5, \frac{1}{3}) \quad \}$.

Cardinality of $\mathbb{Q}$

Example

The rational numbers are countable: There exists an enumeration that assigns to every element of $\mathbb{Q}$ a unique element of $\mathbb{N}$.

Proof (direct by construction).

We demonstrate that the rationals are countable by constructing an enumeration. Create a table with numerators across the top and denominators down the sides:

$\mathbb{Q}$	1	2	3...
1	1/1	2/1	3/1...
2	1/2	2/2	3/2...
3	1/3	2/3	3/3...
⋮			

Start at the top-left and zig-zag across the table, counting fully-reduced fractions as you go: $\{(1, \frac{1}{1}), (2, \frac{2}{1}), (3, \frac{1}{2}), (4, \frac{3}{2}), (5, \frac{1}{3}), \ldots\}$. □

Density of $\mathbb{Q}$ in $\mathbb{R}$

Theorem

For any $a, b \in \mathbb{R}$ where $a < b$, there is a $q \in \mathbb{Q}$ such that $a < q < b$.

Proof (direct by construction).

Let $n = \frac{1}{b-a} + 1$. Then $nb - na > 1$.
Let m be the largest integer such that $m < na$. Then it must be that $na < m + 1 < nb$, since

- $m + 1 < na$ would contradict m being the largest integer less than na, and
- $m + 1 > nb$ cannot be true since $nb - na > 1$.

Hence $a < \frac{m+1}{n} < b$. □

Density and continuous functions

Theorem

If $f : \mathbb{R} \mapsto \mathbb{R}$ *and* $g : \mathbb{R} \mapsto \mathbb{R}$ *are both continuous and* $f(q) = g(q)\ \forall q \in \mathbb{Q}$, *then* $f(x) = g(x)\ \forall x \in \mathbb{R}$.

Density and continuous functions

Theorem

If $f : \mathbb{R} \mapsto \mathbb{R}$ *and* $g : \mathbb{R} \mapsto \mathbb{R}$ *are both continuous and* $f(q) = g(q)\ \forall q \in \mathbb{Q}$, *then* $f(x) = g(x)\ \forall x \in \mathbb{R}$.

Proof.

Assume for contradiction that $f(q) = g(q)\ \forall q \in \mathbb{Q}$, but there exists $a \in \mathbb{R}$ such that $f(a) \neq g(a)$. Let $\epsilon = |f(a) - g(a)|/2$.

Density and continuous functions

Theorem

If $f : \mathbb{R} \mapsto \mathbb{R}$ and $g : \mathbb{R} \mapsto \mathbb{R}$ are both continuous and $f(q) = g(q)\ \forall q \in \mathbb{Q}$, then $f(x) = g(x)\ \forall x \in \mathbb{R}$.

Proof.

Assume for contradiction that $f(q) = g(q)\ \forall q \in \mathbb{Q}$, but there exists $a \in \mathbb{R}$ such that $f(a) \neq g(a)$. Let $\epsilon = |f(a) - g(a)|/2$.
By continuity, there exist $\delta_1, \delta_2 > 0$ such that
$|x - a| < \delta_1$ guarantees $|f(x) - f(a)| < \epsilon$, and
$|x - a| < \delta_2$ guarantees $|g(x) - g(a)| < \epsilon$.

Density and continuous functions

Theorem

If $f : \mathbb{R} \mapsto \mathbb{R}$ *and* $g : \mathbb{R} \mapsto \mathbb{R}$ *are both continuous and* $f(q) = g(q)\ \forall q \in \mathbb{Q}$, *then* $f(x) = g(x)\ \forall x \in \mathbb{R}$.

Proof.

Assume for contradiction that $f(q) = g(q)\ \forall q \in \mathbb{Q}$, but there exists $a \in \mathbb{R}$ such that $f(a) \neq g(a)$. Let $\epsilon = |f(a) - g(a)|/2$.
By continuity, there exist $\delta_1, \delta_2 > 0$ such that
$|x - a| < \delta_1$ guarantees $|f(x) - f(a)| < \epsilon$, and
$|x - a| < \delta_2$ guarantees $|g(x) - g(a)| < \epsilon$.
Choose $q \in \mathbb{Q}$ such that $|q - a| < \min\{\delta_1, \delta_2\}$. (exists by density)

Density and continuous functions

Theorem

If $f : \mathbb{R} \mapsto \mathbb{R}$ *and* $g : \mathbb{R} \mapsto \mathbb{R}$ *are both continuous and* $f(q) = g(q)\ \forall q \in \mathbb{Q}$*, then* $f(x) = g(x)\ \forall x \in \mathbb{R}$*.*

Proof.

Assume for contradiction that $f(q) = g(q)\ \forall q \in \mathbb{Q}$, but there exists $a \in \mathbb{R}$ such that $f(a) \neq g(a)$. Let $\epsilon = |f(a) - g(a)|/2$.
By continuity, there exist $\delta_1, \delta_2 > 0$ such that
$|x - a| < \delta_1$ guarantees $|f(x) - f(a)| < \epsilon$, and
$|x - a| < \delta_2$ guarantees $|g(x) - g(a)| < \epsilon$.
Choose $q \in \mathbb{Q}$ such that $|q - a| < \min\{\delta_1, \delta_2\}$. (exists by density)

$$|f(a) - g(a)| \leq |f(a) - f(q)| + |f(q) - g(q)| + |g(q) - g(a)|$$

Density and continuous functions

Theorem

If $f : \mathbb{R} \mapsto \mathbb{R}$ and $g : \mathbb{R} \mapsto \mathbb{R}$ are both continuous and $f(q) = g(q)\ \forall q \in \mathbb{Q}$, then $f(x) = g(x)\ \forall x \in \mathbb{R}$.

Proof.

Assume for contradiction that $f(q) = g(q)\ \forall q \in \mathbb{Q}$, but there exists $a \in \mathbb{R}$ such that $f(a) \neq g(a)$. Let $\epsilon = |f(a) - g(a)|/2$.
By continuity, there exist $\delta_1, \delta_2 > 0$ such that
$|x - a| < \delta_1$ guarantees $|f(x) - f(a)| < \epsilon$, and
$|x - a| < \delta_2$ guarantees $|g(x) - g(a)| < \epsilon$.
Choose $q \in \mathbb{Q}$ such that $|q - a| < \min\{\delta_1, \delta_2\}$. (exists by density)

$$\begin{aligned} |f(a) - g(a)| &\leq |f(a) - f(q)| + |f(q) - g(q)| + |g(q) - g(a)| \\ &< \epsilon + 0 + \epsilon = |f(a) - g(a)|, \end{aligned}$$

a contradiction. □

Density and continuous functions

Theorem

If $f : \mathbb{R} \mapsto \mathbb{R}$ *and* $g : \mathbb{R} \mapsto \mathbb{R}$ *are both continuous and* $f(q) = g(q)$ $\forall q \in D$ *for any dense subset* $D \subseteq \mathbb{R}$, *then* $f(x) = g(x)$ $\forall x \in \mathbb{R}$.

Proof.

Previous proof only used density of $\mathbb{Q}$, no other properties of $\mathbb{Q}$.
So result goes through for any dense subset of $\mathbb{R}$. □

No largest prime

Theorem

There is no largest prime.

No largest prime

Theorem

There is no largest prime.

Lemma

If $n = a \cdot b + 1$*, then neither* a *nor* b *divides* n*.*

Lemma

Any $n \in \mathbb{N}, r > 1$ *can be written as* $p_1 \cdot p_2 \cdot \ldots \cdot p_k$*, where each* p_i *is prime for* $1 \leq i \leq k$*.*

No largest prime

Theorem
There is no largest prime.

Lemma
If $n = a \cdot b + 1$, then neither a nor b divides n.

Lemma
Any $n \in \mathbb{N}, r > 1$ can be written as $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, where each p_i is prime for $1 \leq i \leq k$.

Proof of theorem (by contradiction).
Suppose that there is a finite sequence of all primes $p_1, p_2, \ldots, p_k$.
Let $q = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$.
Then p_i does not evenly divide q for all $i = 1, \ldots, k$ (first lemma).

No largest prime

Theorem
There is no largest prime.

Lemma
If $n = a \cdot b + 1$, then neither a nor b divides n.

Lemma
Any $n \in \mathbb{N}, r > 1$ can be written as $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, where each p_i is prime for $1 \leq i \leq k$.

Proof of theorem (by contradiction).
Suppose that there is a finite sequence of all primes $p_1, p_2, \ldots, p_k$.
Let $q = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$.
Then p_i does not evenly divide q for all $i = 1, \ldots, k$ (first lemma).
But then it is impossible to write q as the product of primes, contradicting the second lemma. □

Thanks!

Additional examples

- Every tree with n vertices has exactly $n - 1$ edges.
- Sum of vertex degrees in any undirected graph is even.