Algebra 1 - Set Theory and Logic

TSS Math Club

Dec 2022

1 Four Fundamental Proof Techniques:

1.1 Direct Proof (Proof by Construction)

In a constructive proof one attempts to demonstrate $P \implies Q$ directly. This is the simplest and easiest method of proof available to us. There are only two steps to a direct proof (the second step is, of course, the tricky part):

- Assume that P is true.
- Use P to show that Q must be true.

1.1.1 Example

Prove odd number + odd number = even number.

P = hypothesis

Q = Conclusion

k = even

l = odd

odd = $2k+1$

odd = $2l+1$

$2k+1+2l+1$

$= 2(k+l+1)$

1.2 Proof by Contradiction

The proof by contradiction is grounded in the fact that any proposition must be either true or false, but not both true and false at the same time. The method of proof by contradiction:

- Assume that P is true.
- Assume that ¬ Q is true
- Use P and ¬ Q to demonstrate a contradiction.

$P \Rightarrow Q$

Assume then P, not Q

1.2.1 Example

if P is right, then Q cannot be wrong, ∴ Q is right

Prove $\sqrt{2}$ is irrational number.

$\sqrt{2}$ is rational

$\sqrt{2} = \frac{p}{q}$, gcd (p, q)

,

$\sqrt{2}q = p$

$2q^2 = p^2$ P even -> $p = 2k$

-> $2q^2 = (2k)^2 = 4k^2$

$q^2 = 2k^2$

q is even

gcd $(p, q) \geq 2$

Prove for a base case

1.3 Proof by Induction

Show n is true, prove n+1 is true

Proof by induction is a very powerful method in which we use recursion to demonstrate an infinite number of facts in a finite amount of space. In order to prove by induction, you need to:

- Show that a propositional form P(x) is true for some basis case.
- Assume that P(n) is true for some n, and show that this implies that P(n + 1) is true.
- Then, by the principle of induction, the propositional form P(x) is true for all n greater or equal to the basis case.

1.3.1 Example

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

let $n=1$

$\frac{1(1+1)}{2} = 1$

Sub for $n+1$

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

$= \frac{n(n+1) + 2(n+1)}{2}$

$= (n+1)[(n+1)+1]$

Similar to $n(n+1)$

1.4 Proof by Contrapositive

From first-order logic we know that the implication $P \implies Q$ is equivalent to $\neg P \implies \neg Q$. The second proposition is called the contrapositive of the first proposition. By saying that the two propositions are equivalent we mean that if one can prove $P \implies Q$ then they have also proved $\neg P \implies \neg Q$, and vice versa.

1.4.1 Example

Prove n^2 even implies n even.

n^2 even = n even

¬n even = n odd

$(\neg n \text{ even})^2$ = n odd

2 Set Theory

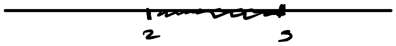
2.1 Definition of a Set:

2.2 Construct a Set

2.2.1 Construct a Set from a List of Ojbects:

$A = \{☺, ☺, 2\} \equiv \{☺, ☺, 2\}$ Note: There is no order in a set.

2.2.2 Construct a Set from a Given Set by Setting Restrictions:



$A = \{x \in \mathbb{R} \mid 2 \leq x \leq 3\}$

2.3 Basic Sets:

Subtract / get rid of

$\mathbb{R}$ = Real $\mathbb{N}$ = integer $\mathbb{R}^+$, $\mathbb{R}_0$, $\mathbb{Q}$, $\mathbb{R} \setminus \mathbb{Q}$

$\mathbb{C}$ = Complex $\mathbb{Z}$

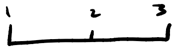
2.4 Relations:

2.4.1 Definition: $x \in A$

x is an <u>element</u> of set A

2.4.2 Definition: $A \subset B$

A is a <u>subset</u> of B



$A = \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}$

$B = \{x \in \mathbb{R} \mid 1 \leq x \leq 3\}$

$1 \in A$

$\{1\} \subset A$

$x \in A \Rightarrow x \in B$

$\therefore A \subset B$

$\neg(x \in A \Rightarrow x \notin B)$

2.4.3 Definition: $A = B$

$\forall x \in A, x \in B$

2.4.4 Lemma: $A = B \iff A \subset B \land B \subset A$

$A = B \Leftrightarrow A \subset B \land B \subset A$

A=B implies A is a subset of B and B is a subset of A

$\neg(x \in A \land x \in B)$ $\land$ = and, $\lor$ = or

$\forall, \exists, \neg, \land, \lor, \in,$

$\neg(x \in A) \lor \neg(x \in B)$

$(x \notin A) \lor (x \notin B)$

$\subset, \subseteq, \subsetneq$

$A = \{1, 2, 3, 4, 5, 6\}$ $A - C = \{4, 5\}$

$C = \{1, 2, 3\}$

2.5 Operations:

$B = \{5, 6, 7, \ldots 11\}$

2.5.1 Definition: $A - B$

The element of x such that x is an element of A and not an element of C.

$$\{x \mid x \in A \land x \notin C\}$$

2.5.2 Definition: $A \cup B$

A union B

$= \{1, 2, 3, 4, 5, 6, 7 \ldots 11\}$

2.5.3 Definition: $A \cap B$

A intersect B

$= \{5, 6, 7\}$

2.6 Ordered Pair:

2.6.1 Definition:

2.6.2 Property:

$(a, b) = \{\{a\}, \{a, b\}\}$ $(a, b) = (c, d) \iff a = c \land b = d$

2.7 Cartesian Product

2.7.1 Definition:

$A = \{1, 2\}$

$B = \{5, 6, 7\}$

$A \times B = \{(x, y) \mid x \in A, y \in B\}$

$A \times B = (1, 5), (1, 6), (1, 7), (2, 5), (2, 6), (2, 7)\}$

3 Relation and Function

3.1 Relation

3.1.1 Definition:

A relation of $f : A \to B$ is subset of $A \times B$

3.2 Function

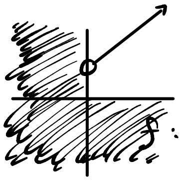
3.2.1 Definition:

(when not stated, $\mathbb{R} \to \mathbb{R}$, $f : \mathbb{R} \to \mathbb{R}$)

- Function
- Domain $f : \underset{\text{Domain}}{\underset{\uparrow}{A}} \to \underset{\text{codomain}}{\underset{\uparrow}{B}}$
- Codomain
- Range where the function actually maps

$f(x) = x + 1$

Range: $\{y \in \mathbb{R} \mid 1 < y\}$



$f : \mathbb{R}^+ \to \mathbb{R}^+$

3.2.2 Injection (one-to-one):

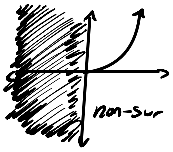
Injection = 1 to 1 input.

for every 1 output, there is 1 input

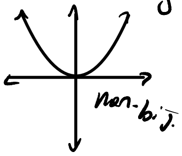
$f : \mathbb{R}_0 \to \mathbb{R}$

$f(x) = x^2$

injection



not injection

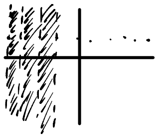


$f : \mathbb{R} \to \mathbb{R}$

$f(x) = x^2$

$g(x) = 1$

$g = z \to \mathbb{R}$

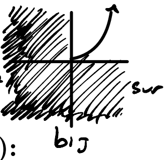


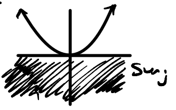
3.2.3 Surjection (onto):

No holes in codomain that aren't covered by range.

$f : \mathbb{R}_0 \to \mathbb{R}_0$

$f(x) = x^2$





$f : \mathbb{R} \to \mathbb{R}_0$

3.2.4 Bijection (one-to-one and onto):

Both surjection and injection

3.2.5 Inverse Function:

$f \qquad g$

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

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h = g \circ f"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

$$\begin{tikzcd} A \arrow[r, shift left, "f"] & B \arrow[l, shift left, "f^{-1}"] \end{tikzcd}$$

$f \circ f^{-1} = f^{-1} \circ f = I_A$

$10^{\log x} = x$

$\log 10^x = x$

4 Cardinality

4.1 Index Set J_n

$J_n \{ 1, 2, 3, -n \}$

4.2 Cardinlity of Finite Set

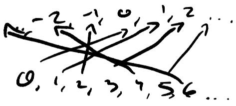
$J_n \xrightarrow[\text{bijection}]{} S \qquad |S| = n$

Must count without skipping values and

Must count all individuals.

4.3 Infinite Countable Set

$\mathbb{N} \xrightarrow[\text{bijection}]{} S$



$Q = \frac{p}{q}$

	1	2	3	4 ...
1	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$ ...
2	$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$ ...
3	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$ ...
4	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$ ...
⋮	⋮	⋮	⋮	⋮

$\therefore |Q| = |Q_+| = |\mathbb{Z}| = |\mathbb{N}|$

4.4 Infinite Uncountable Set

4.5 Two Sets with the Same Cardinality

Prove $\mathbb{R}$ cannot be counted

$\mathbb{R}$

$\mathbb{Z}$

1	$1.\underline{2}3313 42$ — ...
2	$0.2\underline{9}75621$ — ...
3	$1.19\underline{7}6631$ — ...
4	$0.766\underline{3}951$ — ...
5	—
6	—

if 7, change to 0

if not 7, convert to 7

$\therefore 0.7707 \ldots$