# (Defn)

**Set:** set $S$ is collection of things. Every thing $x$ is either $x \in S$ or $x \notin S$

**empty set:** empty set is a set that $\forall x$, $x \notin \emptyset$ $(\{\}$ or $\emptyset)$

**set comprehension:** $A := \{x \mid \text{property of } x\}$ if $x \notin A$, $x \notin B$

**set equality**
- : two sets $A$ and $B$ are equal if $A \subseteq B$ and $B \subseteq A$
- : two sets $A$ and $B$ are equal if $\forall x \in A$, $x \in B$ and $\forall x \in B$, $x \in A$
- : two sets $A$ and $B$ are equal if $\forall x \in A$, iff $x \in B$

**functions:** two sets $A$ and $B$, function $f: A \to B$ is unambiguous. $\forall x \in A$, $\exists y \in B$. ($A$ is domain, $y$ is codomain)

**partial function:** $f: A \nrightarrow B$ is a subset $S \subseteq A$, along with $\tilde{f}: S \to B$
$f(x) = y$ if $\hat{f}(x) = y$ and $f(x)$ is undefined if $x \notin S$.

**total:** partial function $f$ is total if $S$ is equal to domain. I.e $f$ is a function.

**function equality:** two functions $f$ and $g: A \to B$ are equal if they agreen on every input. I.e, $f = g$ if $\forall x \in A$, $f(x) = g(x)$.

$A^c$ = universe

**set operations**
- **Union:** If $A$ and $B$ are sets, $A \cup B := \{x \mid x \in A \text{ or } x \in B\}$
- **Intersection:** If $A$ and $B$ are sets, $A \cap B := \{x \mid x \in A \text{ and } x \in B\}$
- **Set difference:** If $A$ and $B$ are sets, $A \setminus B := \{x \mid x \in A \text{ and } x \notin B\}$

**power set:** $2^A$ is set of all subsets of $A$. $2^A := \{B \mid B \subseteq A\}$.
$\forall$ set $X$, $\exists\, \emptyset \in 2^X$ and $X \in 2^X$

**injectivity:** $f: A \to B$ is injective, if $\forall x_1$ and $x_2 \in A$, whenever $f(x_1) = f(x_2)$, we have $x_1 = x_2$

**surjectivity:** $f: A \to B$ is surjective, if $\forall y \in B$, $\exists x \in A$ such that $f(x) = y$

**bijectivity:** $f: A \to B$ is both injective and surjective

**Identity function**: If $A$ is a set, function $id: A \to A$ given by $id(x) := x$

**composition**: $f: A \to B$ and $g: B \to C$, $g \circ f: A \to C$, given by $(g \circ f)(a) := g(f(a))$

**left inverse**: $f: A \to B$, left inverse $g$ of $f$ is $g: B \to A$ satisfying $g \circ f = id$

i.e $\forall x \in A$, $g(f(x)) = x$.

**right inverse**: $f: A \to B$, a right inverse $g$ of $f$ is a $g: B \to A$ satisfying $f \circ g = id$

i.e $\forall x \in B$, $f(g(x)) = x$

**two-sided inverse**: If $f: A \to B$, $g: B \to A$ is a two-sided inverse of $f$

if $f \circ g = id_B$ and $g \circ f = id_A$

**Cardinality**: size of a set

- **$\le$**: If $A$ and $B$ are sets, then $|A| \le |B|$ means $\exists$ injection $f: A \to B$
- **$\ge$**: If $A$ and $B$ are sets, then $|A| \ge |B|$ means $\exists$ surjection $f: A \to B$
- **$=$**: If $A$ and $B$ are equal, then $|A| = |B|$ means $\exists$ bijection $f: A \to B$

If $|N| \ge |X|$, then $X$ is countable

**Countable**: If $|X| \le |N|$, then a set $X$ is countable

i.e If $\exists$ a surjection $f: N \to X$, then $X$ is countable

inequalities $(\le, <, \ge)$
subsets $(\subseteq, \supseteq)$

equation $x+y=z$ means $(x,y,z) \in \mathbb{R}$ iff $x+y=z$

**Relation**: A relation $R$ on sets $A_1, A_2, A_3 \ldots A_n$ is a subset of $A_1 \times A_2 \cdots \times A_3$

**Binary relation**: A binary relation $R$ on a set $A$ is a subset of $A \times A$

ex) $xRy$ means $(x,y) \in R$, $x \le y$ means $(x,y) \in \le$, $f(x) = y$ means $(x,y) \in f$

- **Reflexity**: A binary relation $R$ is reflexive if $\forall x \in R$, $xRx$
- **Symmetry**: A binary relation $R$ is symmetry if $\forall$ pairs of elements $x, y \in A$ $xRy$, $\exists\, yRx$
- **Transitivity**: A binary relation $R$ is transitive if $\forall\, x, y, z \in R$ $xRy$ and $yRz$, $\exists\, xRz$

**Equivalnce Relation**: A binary relation $R$ is equivalence relation if $R$ is reflexive, symmetry, and transitive

# (proof)

table of proof techniques:

case 1: P is true
R is true?
case 2: Q is true
R is true?

| Proposition | Symbol | To prove it | To use it | Logical negation |
|---|---|---|---|---|
| P and Q | (P ∧ Q) | prove both P and Q | you may use either P or Q | (¬P) ∨ (¬Q) |
| P or Q | (P ∨ Q) | You may either prove P or prove Q | case analysis | (¬P) ∧ (¬Q) |
| P is false (or "not P") | ¬ P | disprove P | contradiction | P |
| if P then Q (or "P implies Q") | P ⇒ Q | assume P, then prove Q | if you know P, conclude Q | P ∧ ¬ Q |
| for all x, P | ∀x, P | choose an arbitrary value x | apply to a specific x | ∃ x, ¬ P |
| there exists x such that *P* | ∃x, P | give a specific x | use an arbitrary x satisfying P | ∀ x, ¬ P |

proof: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

- choose an arb set A, B, and C
- WTS that LHS ⊆ RHS and RHS ⊆ LHS
  - To show LHS ⊆ RHS, choose an arb $x \in$ LHS
  - $x \in A$ or $x \in (B \cap C)$
    - Since $x \in A$, $x \in (A \cup B)$ and $x \in (A \cup C)$
    - therefore $x \in$ RHS
    - since $x \in (B \cap C)$, $x \in (A \cup B)$ because $x \in B$ and $x \in (A \cup C)$ because $x \in C$
    - therfore LHS ⊆ RHS
  - To show RHS ⊆ LHS, Choose an arb $x \in$ RHS
  - Since $x \in (A \cup B)$ and $x \in (A \cup C)$, so either $x \in A$ or $x \notin A$
    - If $x \in A$, then $x \in$ LHS
    - If $x \notin A$, then x must be in B and C. So $x \in (B \cap C)$, $x \in$ LHS
    - therefore RHS ⊆ LHS
- So LHS = RHS

proof: If $A = \emptyset$ and $f: A \to B$ is injective, then $f$ has a left inverse

- Assume that $f: A \to B$ is injective
  - i.e $\forall x_1$ and $x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$
- WTS that $\exists$ left inverse $g$ of $f$
  - i.e that $g \circ f = \mathrm{id}$
  - let $g(y) := x$
  - choose an arb $x_0 \in A$, let $y = f(x_0)$
  - By defn of $g$, $g(y) = x_0$
  - i.e $g(f(x)) = x_0$
  - so $g \circ f = \mathrm{id}$, $\exists$ left inverse $g$

proof: If $f: A \to B$ has a left inverse $g: B \to A$, then $f$ is injective

- Assume that $f: A \to B$ has a left inverse $g: B \to A$
  - i.e that $g \circ f = \mathrm{id}$
- WTS that $f$ is injective.
  - i.e WTS that $\forall x_1$ and $x_2 \in A$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.
  - choose an arb $x_1$ and $x_2$, assume $f(x_1) = f(x_2)$. WTS that $x_1 = x_2$.
  - since $g \circ f = \mathrm{id}$, $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$
  - so $x_1 = x_2$, $f$ is injective

proof: If $f: A \to B$ is surjective, then $f$ has a right inverse

- Assume that $f: A \to B$ is surjective
  - i.e $\forall y \in B$, $\exists x \in A$ such that $f(x) = y$
- WTS that $\exists$ right inverse $g$ of $f$
  - i.e $f \circ g = id$
  - let $g(y) := x$
  - choose an arb $y \in B$
  - $(f \circ g)(y) = f(x) = y$

    $f \circ g = id$
- so $g$ is a right inverse of $f$

proof: If $f: A \to B$ has a right inverse $g: B \to A$ then $f$ is a surjective

- Assume that $f: A \to B$ has a right inverse $g: B \to A$
  - i.e $f \circ g = id$
- WTS that $f$ is surjective
  - i.e $\forall y \in B$, $\exists x \in A$ such that $f(x) = y$
  - choose an arb $y$, $y = f(x)$
  - let $x = g(y)$
  - $(f \circ g)(y) = f(g(y)) = f(x) = y$
  - so $f$ is surjective

proof: If $f: A \to B$ is a bijection, then $f$ has a two-sided inverse proof: $\forall$ set $A$, we have $|A| \leq |A|$ reflexive

- choose an arb set $A$
- WTS that $\exists f: A \to A$ is injective
  - i.e $\forall x_1, x_2 \in A$, If $f(x_1) = f(x_2)$ then $x_1 = x_2$
  - choose an arb $x_1$ and $x_2$
  - assume $id(x_1) = id(x_2)$, then $x_1 = id(x_1) = id(x_2) = x_2$
  - so $x_1 = x_2$
  - $\exists f$ is Injective

proof: If $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$ transitive

- Assume $|A| \leq |B|$ and $|B| \leq |C|$
  - i.e $\exists f: A \to B$ is injective and $\exists g: B \to C$ is Injective
- WTS that $|A| \leq |C|$
  - i.e $\exists g \circ f: A \to C$ is injective
  - i.e $\forall x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$
  - choose arb $x_1$ and $x_2 \in A$
  - assume $g \circ f(x_1) = g \circ f(x_2)$
  - WTS that $x_1 = x_2$
  - since $g$ is injective, $f(x_1) = f(x_2)$ and $f$ is injective, $x_1 = x_2$
  - so $x_1 = g(f(x_1)) = g(f(x_2)) = x_2$

proof: $|A| \leq |B|$ iff $|B| \geq |A|$ Symmetry .

- Given $|A| \leq |B|$ then $|B| \geq |A|$
- Since $|A| \leq |B|$, $\exists f: A \to B$ that is injective
  - since $f$ is injective, $\exists$ left inverse $g$ of $f$
- WTS that $\exists g: B \to A$ that is surjective
  - since $g$ is a left inverse of $f$, $f$ is a right inverse of $g$.
  - since $g$ has a right inverse, $g$ is surjective.

proof: If $|A| \leq |B|$ and $|A| \geq |B|$ then $|A| = |B|$

proof: $|N \cup (-1)| = |N|$, if $f: |N| \rightarrow |N \cup (-1)|$, then $f$ is bijective

- Assume $f(n) := n-1$
- WTS that $f$ is bijective
  - I.e $f$ is injective
    - choose an arb $x_1$ and $x_2 \in A$
    - assume $f(x_1) = f(x_2)$, then $x_1 = x_2$
    - $x_1 = x_1 - 1 = x_2 - 1 = x_2$, so $x_1 = x_2$
  - I.e $f$ is surjective
    - choose an arb $y \in RHS$
    - let $x = y+1$, WTS $f(x) = y$
    - $y \geq -1$, so $x \geq 0$
    - so $f(x) = x - 1 = y$
- so $f$ is bijective

proof: Let $X := \{2n \mid n \in N\}$ be the set of even natural numbers. Then $|X| = |N|$

proof: $|Z| = |N|$

proof: $|N \times N| = N$

- Assume $f: N \rightarrow |N \times N|$
- WTS that $f$ is bijective
  - I.e enumerate each pair exactly once

| | 0 | 1 | 2 | .. |
|---|---|---|---|---|
| 0 | (0,0) | (0,1) | (0,2) | |
| 1 | (1,0) | (1,1) | (1,2) | |
| 2 | (2,0) | (2,1) | (2,2) | |
| : | | | | |

| n | f(n) |
|---|---|
| 0 | (0,0) |
| 1 | (1,0) |
| 2 | (0,1) |
| 3 | (2,0) |
| 4 | (1,1) |
| 5 | (0,2) |
| : | : |

- pattern hits each pair once, so $f$ is bijective proof : (Diagnolization) $2^N$ is uncountable

- For sake of Contradiction, if $2^N$ is countable, then $\exists$ surjection $f: N \to 2^N$
-

| i | f(i) | $0 \in f(i)$? | $1 \in f(i)$? | $2 \in f(i)$? | $3 \in f(i)$? | $4 \in f(i)$? | ⋯ |
|---|---|---|---|---|---|---|---|
| 0 | $\mathbb{N}$ | (yes) | yes | yes | yes | yes | ⋯ |
| 1 | $\emptyset$ | no | (no) | no | no | no | ⋯ |
| 2 | the set of even numbers | yes | no | (yes) | no | yes | ⋯ |
| 3 | the set of odd numbers | no | yes | no | (yes) | no | ⋯ |
| 4 | $\{1\}$ | yes | no | no | no | (no) | ⋯ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |

this construction work for an arb f

- Construct a new diabolic set $S_D$ by changing each element on the diagnol

| | $0 \in f(i)$? | $1 \in f(i)$? | $2 \in f(i)$? | $3 \in f(i)$? | $4 \in f(i)$? | ⋯ |
|---|---|---|---|---|---|---|
| $S_D$ | no | yes | no | no | yes | ⋯ |

- $i \in S_D$ iff $i \notin f(i)$
  - i.e $S_D := \{i \mid i \notin f(i)\}$
- Since $\forall k$, $S_D$ differs from $f(k)$ in $k$th column, $S_D$ cannot be in the image of $f$
- If $k \in f(k)$ then $k \notin S_D$, and $k \notin f(k)$ then $k \in S_D$
  - So, $S_D \neq f(k)$
- Thus, $f$ is not surjective, a contradiction

proof : (Diagnolization) $\mathbb{R}$ is uncountable

- For sake of Contradiction, if $I$ is countable, then $\exists$ surjection $f: N \to I$
- Let $I = [0, 1)$, $I \subseteq \mathbb{R}$

| i | f(i) | tenths | hundredths | thousandths | ⋯ | ⋯ | ⋯ |
|---|---|---|---|---|---|---|---|
| 0 | 1/2 | (5) | 0 | 0 | 0 | 0 | ⋯ |
| 1 | 0 | 0 | (0) | 0 | 0 | 0 | ⋯ |
| 2 | $\pi - 3$ | 1 | 4 | (1) | 5 | 9 | ⋯ |
| 3 | $0.8989\cdots$ | 8 | 9 | 8 | (9) | 8 | ⋯ |
| 4 | 1/2 | 5 | 0 | 0 | 0 | (0) | ⋯ |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |

- Construct a new diabolic set $S_D$ by adding 5 to each digit, $X_D = 0.05645$
- If $k \in f(k)$ then $k \notin S_D$, and $k \notin f(k)$ then $k \in S_D$
  - So, $S_D \neq f(k)$
- Thus, $f$ is not surjective, a contradiction