Functions and its properties

Let A, B be two nonempty sets.
The cartesian product of A and B is

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

Note: $A \times B \neq B \times A$.
Let $A = \{1, 2, 3\}$, $B = \{a, b\}$. Then
$A \times B = \{(1, a), (2, a), (3, a), (1, b), (2, b), (3, b)\}$

Definition (Function)

A function f from A to B is an assignment for each element a of A, a unique element b of B. $a \rightsquigarrow b$
A function f from A to B is a subset of $A \times B$ such that for each $a \in A$, there exists unique $b \in B$ such that $(a, b) \in f$.

Notation: $f : A \to B$: a function f from A to B
for each $(a, b) \in f$, we write $f(a) = b$.

Examples of function

- Let $A = \{a, b\}$ and $\{1, 2, 3\}$. Then

  $$f = \{(a, 2), (b, 3)\}$$

  is a function; whereas

  $$g = \{(a, 1), (a, 2), (b, 1)\}$$

  is not a function.
- Let $A = B = \mathbb{R}$ and $f(x) = x^2$. Then $f : \mathbb{R} \to \mathbb{R}$ is a function. Define $g : \mathbb{R} \to \mathbb{R}$ as $g(x) := y$, if $y^2 = x$. Then g is not a function from $\mathbb{R}$ to $\mathbb{R}$.
- Let A be a non-empty set. The identity function on A, 1_A is defined as $1_A(a) = a$ for all $a \in A$.

Definition

Suppose

$$f : A \to B$$

$$g : B \to C$$

are functions. The composite of f and g, $g \circ f : A \to C$ is a function defined as

$$g \circ f(a) := g(f(a)) \text{ for each } a \in A.$$

Let $f : A \to B$ be a function.
Domain of f=A.
Codomain of f=B.
Range of $f = \{b \in B | f(a) = b \text{ for some } a \in A\}$
f is said to be onto/surjective if Range of $f = B$.
f is said to be injective if $f(a) = f(a')$ then $a = a'$

Define $f, g : \mathbb{R} \to \mathbb{R}$ as

$$f(x) = x^2,$$

$$g(x) = +\sqrt{|x|}$$

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

What is $f \circ g$?

Theorem

Let $f, g : \mathbb{R} \to \mathbb{R}$ be two functions. Suppose $g \circ f$ is injective. Then f is injective

Proof.

Let $f(a) = f(a')$.
We need to prove $a = a'$
Hence $g(f(a)) = g(f(a'))$, i.e., $g \circ f(a) = g \circ f(a')$
Since $g \circ f$ is injective, $a = a'$. $\square$

Let $f : A \to B$ be a function,i.e.,

$$f = \{(a, f(a)) | a \in A\}$$

Consider the set

$$g = \{(f(a), a) | a \in A\} \subseteq B \times A$$

If g is a function from B to A, then f is said to be invertible with $f^{-1} = g$.
Note: $f \circ f^{-1} = 1_B$ and $f^{-1} \circ f = 1_A$
Example: Let $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$.
$f = \{(a, 2), (b, 1), (c, 2)\}$
Is f invertible?

Let $f : A \to B$ be a function,i.e.,

$$f = \{(a, f(a)) | a \in A\}$$

Consider the set

$$g = \{(f(a), a) | a \in A\} \subseteq B \times A$$

If g is a function from B to A, then f is said to be invertible with $f^{-1} = g$.
Note: $f \circ f^{-1} = 1_B$ and $f^{-1} \circ f = 1_A$
Example: Let $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$.
$f = \{(a, 2), (b, 1), (c, 2)\}$
Is f invertible? No.
Is $g = \{(a, 2), (b, 1), (c, 3)\}$ invertible?

Let $f : A \to B$ be a function,i.e.,

$$f = \{(a, f(a)) | a \in A\}$$

Consider the set

$$g = \{(f(a), a) | a \in A\} \subseteq B \times A$$

If g is a function from B to A, then f is said to be invertible with $f^{-1} = g$.
Note: $f \circ f^{-1} = 1_B$ and $f^{-1} \circ f = 1_A$
Example: Let $A = \{a, b, c\}$ and $B = \{1, 2, 3\}$.
$f = \{(a, 2), (b, 1), (c, 2)\}$
Is f invertible? No.
Is $g = \{(a, 2), (b, 1), (c, 3)\}$ invertible? Yes.

Theorem (Criteria for invertible functions)

A function $f : A \to B$ *is invertible if and only if* f *is injective and onto.*

Theorem (Criteria for invertible functions)

A function $f : A \to B$ is invertible if and only if f is injective and onto.

Proof.

Let f be invertible.
Since $f^{-1} : B \to A$ is a function, Domain of $f^{-1} = B$.
Hence Range of $f = B$, i.e., f is onto.

Theorem (Criteria for invertible functions)

A function $f : A \to B$ is invertible if and only if f is injective and onto.

Proof.

Let f be invertible.
Since $f^{-1} : B \to A$ is a function, Domain of $f^{-1} = B$.
Hence Range of $f = B$, i.e., f is onto.
Let $f(a) = f(a')$
Since f^{-1} is a function,

$$f^{-1}(f(a)) = f^{-1}(f(a'))$$

$$\text{i.e., } a = a'$$

□

Theorem

Let A and B be two nonempty finite sets of same cardinality and $f : A \to B$ be a function. If f is injective, then f is invertible.

Theorem

Let A and B be two nonempty finite sets of same cardinality and $f : A \to B$ be a function. If f is injective, then f is invertible.

Proof.

Let $A = \{a_1, \cdots, a_n\}$.
Since f is injective, $f(a_1), f(a_2), \cdots, f(a_n)$ are all distinct elements of B.
But $|B| = |A| = n$. Hence

$$B = \{f(a_1), f(a_2), \cdots, f(a_n)\}, \text{ i.e., } f \text{ is onto.}$$

$\square$

Theorem

Let A and B be two nonempty finite sets of same cardinality and $f : A \to B$ be a function. If f is injective, then f is invertible.

Proof.

Let $A = \{a_1, \cdots, a_n\}$.
Since f is injective, $f(a_1), f(a_2), \cdots, f(a_n)$ are all distinct elements of B.
But $|B| = |A| = n$. Hence

$$B = \{f(a_1), f(a_2), \cdots, f(a_n)\}, \text{ i.e., } f \text{ is onto.}$$

$\square$

Theorem

Let A and B be two nonempty finite sets of same cardinality and $f : A \to B$ be a function. If f is surjective, then f is invertible.

Application of invertible functions in Cryptography

Let $A = \{a, b, \cdots, z\}$ and $f : A \to A$ be an invertible function.
Take a message. Encode the message by replacing each alphabet of it by its image under f.
(In order to decode this encoded message, f must have inverse.)
The recipient decodes the message by applying f^{-1} to each alphabet.

Graph of a function

Definition (Graph of a function)

Let $f : A \to B$ be a function. The graph of f is the set of ordered pairs

$$\{(a, f(a)) | a \in A\}$$

Graph of a function

Definition (Graph of a function)

Let $f : A \to B$ be a function. The graph of f is the set of ordered pairs

$$\{(a, f(a)) | a \in A\}$$

Question: Display the graph of a function $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(n) = n^2$.

Sequence is a ordered list of elements.

Definition (Sequence)

A sequence of the set S is a function

$$a : A \to S \quad \text{where } A \subseteq \mathbb{N}$$

We will write it as $(a_n)_{n=1}^{\infty}$, where $a_n = a(n)$, n^{th} term of the sequence.

Sequence is a ordered list of elements.

Definition (Sequence)

A sequence of the set S is a function

$$a : A \to S \quad \text{where } A \subseteq \mathbb{N}$$

We will write it as $(a_n)_{n=1}^{\infty}$, where $a_n = a(n)$, n^{th} term of the sequence.

Examples:

1. $a_n = \frac{1}{n}$ sequence of rational numbers.

Sequences and summations

Sequence is a ordered list of elements.

Definition (Sequence)

A sequence of the set S is a function

$$a : A \to S \quad \text{where } A \subseteq \mathbb{N}$$

We will write it as $(a_n)_{n=1}^{\infty}$, where $a_n = a(n)$, n^{th} term of the sequence.

Examples:

1. $a_n = \frac{1}{n}$ sequence of rational numbers.
2. (Arithmetic progression) $\{a, a+d, a+2d, a+3d, ...\}$. n^{th} term is $a + (n-1)d$

Sequences and summations

Sequence is a ordered list of elements.

Definition (Sequence)

A sequence of the set S is a function

$$a : A \to S \quad \text{where } A \subseteq \mathbb{N}$$

We will write it as $(a_n)_{n=1}^{\infty}$, where $a_n = a(n)$, n^{th} term of the sequence.

Examples:
1. $a_n = \frac{1}{n}$ sequence of rational numbers.
2. (Arithmetic progression) $\{a, a+d, a+2d, a+3d, ...\}$. n^{th} term is $a+(n-1)d$
3. (Geometric progression) $\{a, ar, ar^2, ar^3, ...\}$. n^{th} term is $ar^{(n-1)}$

Task: Given first few terms of the sequence, identify the remaining terms:
$\{1, \frac{1}{2}, \frac{1}{3}, \ldots\}$ be a sequence. n^{th} term of the sequence is

Task: Given first few terms of the sequence, identify the remaining terms:

$\{1, \frac{1}{2}, \frac{1}{3}, \dots\}$ be a sequence. n^{th} term of the sequence is $\frac{1}{n}$.
$\{6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \dots\}$ be a sequence. n^{th} term of the sequence is

Task: Given first few terms of the sequence, identify the remaining terms:

$\{1, \frac{1}{2}, \frac{1}{3}, \ldots\}$ be a sequence. n^{th} term of the sequence is $\frac{1}{n}$.

$\{6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \ldots\}$ be a sequence. n^{th} term of the sequence is $\frac{2}{3^{n-2}}$.

$\{2, 6, 18, 54, 162, \ldots\}$ be a sequence. Then n^{th} term of the sequence is

Task: Given first few terms of the sequence, identify the remaining terms:

$\{1, \frac{1}{2}, \frac{1}{3}, \ldots\}$ be a sequence. n^{th} term of the sequence is $\frac{1}{n}$.

$\{6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \ldots\}$ be a sequence. n^{th} term of the sequence is $\frac{2}{3^{n-2}}$.

$\{2, 6, 18, 54, 162, \ldots\}$ be a sequence. Then n^{th} term of the sequence is $2.(3)^{n-1}$.

Let $\{a_n\}_{n=1}^{\infty}$ be a sequence.

$$\sum_{i=m}^{n} a_i := a_m + a_{m+1} + \cdots + a_n$$

Let $\{a_n\}_{n=1}^{\infty}$ be a sequence.

$$\sum_{i=m}^{n} a_i := a_m + a_{m+1} + \cdots + a_n$$

$$\sum_{i=m}^{n} (a_i + b_i) = \sum_{i=m}^{n} (a_i) + \sum_{i=m}^{n} (b_i)$$

Let $\{a_n\}_{n=1}^{\infty}$ be a sequence.

$$\sum_{i=m}^{n} a_i := a_m + a_{m+1} + \cdots + a_n$$

$$\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n}(a_i) + \sum_{i=m}^{n}(b_i)$$

$$\sum_{i=m}^{n}(ca_i) = c\sum_{i=m}^{n}(a_i), \text{ where c is a constant}$$

Let $\{a_n\}_{n=1}^{\infty}$ be a sequence.

$$\sum_{i=m}^{n} a_i := a_m + a_{m+1} + \cdots + a_n$$

$$\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n}(a_i) + \sum_{i=m}^{n}(b_i)$$

$$\sum_{i=m}^{n}(ca_i) = c\sum_{i=m}^{n}(a_i), \text{ where c is a constant}$$

$$\sum_{i=1}^{4}\sum_{j=2}^{3} ij = \sum_{i=1}^{4} 2i + 3i = (2+3)+(4+6)+(6+9)+(8+12) = 50$$

Let $\{a_n\}_{n=1}^{\infty}$ be a sequence.

$$\sum_{i=m}^{n} a_i := a_m + a_{m+1} + \cdots + a_n$$

$$\sum_{i=m}^{n}(a_i + b_i) = \sum_{i=m}^{n}(a_i) + \sum_{i=m}^{n}(b_i)$$

$$\sum_{i=m}^{n}(ca_i) = c\sum_{i=m}^{n}(a_i), \text{ where c is a constant}$$

$$\sum_{i=1}^{4}\sum_{j=2}^{3} ij = \sum_{i=1}^{4} 2i+3i = (2+3)+(4+6)+(6+9)+(8+12) = 50$$

$$\sum_{i=1}^{4}\sum_{j=2}^{3} ij = \sum_{i=1}^{4} i\sum_{j=2}^{3} j = \sum_{i=1}^{4} i(5) = 5(1+2+3+4) = 50$$

Question: Let a, r be real numbers and $r \neq 0, 1$. Find $\sum_{j=0}^{n} ar^j$.

Question: Let a, r be real numbers and $r \neq 0, 1$. Find $\sum_{j=0}^{n} ar^j$.
Let $S = \sum_{j=0}^{n} ar^j$

$$rS = \sum_{j=0}^{n} ar^{j+1}$$

$$= \sum_{k=1}^{n+1} ar^k$$

$$= (\sum_{k=0}^{n} ar^k) + (ar^{n+1} - a)$$

$$rS = S + (ar^{n+1} - a)$$

$$(r-1)S = (ar^{n+1} - a)$$

$$S = \frac{(ar^{n+1} - a)}{r-1} \quad \textit{since} \quad r \neq 1$$

Determine whether each of these functions from $\mathbf{Z}$ to $\mathbf{Z}$ is one-to-one.

a) $f(n) = n - 1$
b) $f(n) = n^2 + 1$
c) $f(n) = n^3$
d) $f(n) = \lceil n/2 \rceil$

Which functions in Exercise 12 are onto?

Determine whether $f: \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ is onto if

a) $f(m, n) = 2m - n$.
b) $f(m, n) = m^2 - n^2$.
c) $f(m, n) = m + n + 1$.
d) $f(m, n) = |m| - |n|$.
e) $f(m, n) = m^2 - 4$.

Infinite sets

We learnt that if A is a finite set then $|A| =$ no. of distinct elements of A.

Infinite sets

We learnt that if A is a finite set then $|A| =$ no. of distinct elements of A.

What about cardinality of infinte sets?

Infinite sets

We learnt that if A is a finite set then $|A| =$ no. of distinct elements of A.

What about cardinality of infinte sets?

We saw

If S is a finite set, then every injective function $f : S \to S$ is surjective.

Infinite sets

We learnt that if A is a finite set then $|A| =$ no. of distinct elements of A.

What about cardinality of infinte sets?

We saw

If S is a finite set, then every injective function $f : S \to S$ is surjective.

This statement is same as

If there exists an injective function $f : S \to S$ which is not surjective, then S is not finite(that is, infinite).

Infinite sets

We learnt that if A is a finite set then $|A| =$ no. of distinct elements of A.

What about cardinality of infinte sets?

We saw

If S is a finite set, then every injective function $f : S \to S$ is surjective.

This statement is same as

If there exists an injective function $f : S \to S$ which is not surjective, then S is not finite(that is, infinite).

Definition

A set S is said to be infinite if there exists an injective function $f : S \to S$ which is not surjective.

Infinite sets

We learnt that if A is a finite set then $|A| =$ no. of distinct elements of A.

What about cardinality of infinte sets?

We saw

If S is a finite set, then every injective function $f : S \to S$ is surjective.

This statement is same as

If there exists an injective function $f : S \to S$ which is not surjective, then S is not finite(that is, infinite).

Definition

A set S is said to be infinite if there exists an injective function $f : S \to S$ which is not surjective.

Example: The sets $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ are infinite sets.

Infinite sets

We learnt that if A is a finite set then $|A| =$ no. of distinct elements of A.

What about cardinality of infinte sets?

We saw

If S is a finite set, then every injective function $f : S \to S$ is surjective.

This statement is same as

If there exists an injective function $f : S \to S$ which is not surjective, then S is not finite(that is, infinite).

Definition

A set S is said to be infinite if there exists an injective function $f : S \to S$ which is not surjective.

Example: The sets $\mathbb{N}, \mathbb{Q}, \mathbb{R}$ are infinite sets.

Definition (countable set)

A set S is said to be countable if either it is finite or if there exists a bijective (injective and surjective) function $f : \mathbb{N} \to S$.

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$

If there exists an injective function $f : A \to B$, then we say $|A| \leq |B|$.

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$
If there exists an injective function $f : A \to B$, then we say $|A| \leq |B|$.
$|A| = |B|$ if and only if there exists a bijective function $f : A \to B$

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$

If there exists an injective function $f : A \to B$, then we say $|A| \leq |B|$.

$|A| = |B|$ if and only if there exists a bijective function $f : A \to B$

Theorem (Schröder-Bernstein-Cantor theorem)

If $f : A \to B$ and $g : B \to A$ are injective functions then there exists a bijective function $h : A \to B$.

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$

If there exists an injective function $f : A \to B$, then we say $|A| \leq |B|$.

$|A| = |B|$ if and only if there exists a bijective function $f : A \to B$

Theorem (Schröder-Bernstein-Cantor theorem)

If $f : A \to B$ and $g : B \to A$ are injective functions then there exists a bijective function $h : A \to B$.

Exercise: Show that $|[0, 1]| = |(0, 1)|$.

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$
If there exists an injective function $f : A \to B$, then we say $|A| \leq |B|$.
$|A| = |B|$ if and only if there exists a bijective function $f : A \to B$

Theorem (Schröder-Bernstein-Cantor theorem)

If $f : A \to B$ and $g : B \to A$ are injective functions then there exists a bijective function $h : A \to B$.

Exercise: Show that $|[0, 1]| = |(0, 1)|$.
If the set A is countably infinite, then

$$|A| = \aleph_0$$

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$
If there exists an injective function $f : A \to B$, then we say $|A| \leq |B|$.
$|A| = |B|$ if and only if there exists a bijective function $f : A \to B$

Theorem (Schröder-Bernstein-Cantor theorem)

If $f : A \to B$ and $g : B \to A$ are injective functions then there exists a bijective function $h : A \to B$.

Exercise: Show that $|[0, 1]| = |(0, 1)|$.
If the set A is countably infinite, then

$$|A| = \aleph_0$$

An infinite set is said to be uncountable if it is not countable.

Cardinality of infinite sets

We define the cardinality of $\mathbb{N} := \aleph_0$
If there exists an injective function $f : A \to B$, then we say $|A| \leq |B|$.
$|A| = |B|$ if and only if there exists a bijective function $f : A \to B$

Theorem (Schröder-Bernstein-Cantor theorem)

If $f : A \to B$ and $g : B \to A$ are injective functions then there exists a bijective function $h : A \to B$.

Exercise: Show that $|[0, 1]| = |(0, 1)|$.
If the set A is countably infinite, then

$$|A| = \aleph_0$$

An infinite set is said to be **uncountable** if it is not countable.
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countable.

Theorem

$\mathbb{R}$ *is uncountable.*

Theorem

$\mathbb{R}$ *is uncountable.*

Proof: Suppose not, i.e., $\mathbb{R}$ is countable.

Theorem

$\mathbb{R}$ *is uncountable.*

Proof: Suppose not, i.e., $\mathbb{R}$ is countable.
Then $[0, 1]$ is also countable.

Theorem

$\mathbb{R}$ *is uncountable.*

Proof: Suppose not, i.e., $\mathbb{R}$ is countable.
Then $[0, 1]$ is also countable.
Let $f : \mathbb{N} \rightarrow [0, 1]$ be a bijection.
$r_1, r_2, r_3, \cdots$ be all real numbers of $[0, 1]$, where $f(n) = r_n$

Theorem

$\mathbb{R}$ *is uncountable.*

Proof: Suppose not, i.e., $\mathbb{R}$ is countable.
Then $[0,1]$ is also countable.
Let $f : \mathbb{N} \to [0,1]$ be a bijection.
$r_1, r_2, r_3, \cdots$ be all real numbers of $[0,1]$, where $f(n) = r_n$
Use Cantor's diagonalization argument as follows:
$r_1 = 0.d_{11}d_{12}d_{13}\cdots$
$r_2 = 0.d_{21}d_{22}d_{23}\cdots$
$r_3 = 0.d_{31}d_{32}d_{33}\cdots$ and so on
Construct $r = 0.d_1d_2d_3d_4\cdots$ as follows:
Choose d_i different from d_{ii} for all i

Theorem

$\mathbb{R}$ *is uncountable.*

Proof: Suppose not, i.e., $\mathbb{R}$ is countable.
Then $[0, 1]$ is also countable.
Let $f : \mathbb{N} \to [0, 1]$ be a bijection.
$r_1, r_2, r_3, \cdots$ be all real numbers of $[0, 1]$, where $f(n) = r_n$
Use Cantor's diagonalization argument as follows:
$r_1 = 0.d_{11}d_{12}d_{13}\cdots$
$r_2 = 0.d_{21}d_{22}d_{23}\cdots$
$r_3 = 0.d_{31}d_{32}d_{33}\cdots$ and so on
Construct $r = 0.d_1d_2d_3d_4\cdots$ as follows:
Choose d_i different from d_{ii} for all i
Then $r \neq r_i$ for any i. $\square$

Theorem

$\mathbb{R}$ *is uncountable.*

Proof: Suppose not, i.e., $\mathbb{R}$ is countable.
Then $[0,1]$ is also countable.
Let $f : \mathbb{N} \to [0,1]$ be a bijection.
$r_1, r_2, r_3, \cdots$ be all real numbers of $[0,1]$, where $f(n) = r_n$
Use Cantor's diagonalization argument as follows:
$r_1 = 0.d_{11}d_{12}d_{13}\cdots$
$r_2 = 0.d_{21}d_{22}d_{23}\cdots$
$r_3 = 0.d_{31}d_{32}d_{33}\cdots$ and so on
Construct $r = 0.d_1d_2d_3d_4\cdots$ as follows:
Choose d_i different from d_{ii} for all i
Then $r \neq r_i$ for any i. $\square$
Define $|\mathbb{R}| := c$

If $|S| = n$ then $|P(S)| = 2^n$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

$$A = \{x | x \notin g(x)\} \in P(S)$$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

$$A = \{x | x \notin g(x)\} \in P(S)$$

Suppose g is surjective.

$$A = g(a) \text{ for some } a \in S$$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

$$A = \{x | x \notin g(x)\} \in P(S)$$

Suppose g is surjective.

$$A = g(a) \text{ for some } a \in S$$
$$a \in A \Leftrightarrow a \in \{x | x \notin g(x)\}$$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

$$A = \{x | x \notin g(x)\} \in P(S)$$

Suppose g is surjective.

$$\begin{aligned} A = g(a) &\text{ for some } a \in S \\ a \in A \Leftrightarrow a &\in \{x | x \notin g(x)\} \\ &\Leftrightarrow a \notin g(a) \end{aligned}$$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

$$A = \{x | x \notin g(x)\} \in P(S)$$

Suppose g is surjective.

$$\begin{gathered} A = g(a) \text{ for some } a \in S \\ a \in A \Leftrightarrow a \in \{x | x \notin g(x)\} \\ \Leftrightarrow a \notin g(a) \\ \Leftrightarrow a \notin A \end{gathered}$$

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

$$A = \{x | x \notin g(x)\} \in P(S)$$

Suppose g is surjective.

$$\begin{gathered} A = g(a) \text{ for some } a \in S \\ a \in A \Leftrightarrow a \in \{x | x \notin g(x)\} \\ \Leftrightarrow a \notin g(a) \\ \Leftrightarrow a \notin A \end{gathered}$$

Contradiction to g is surjective.

If $|S| = n$ then $|P(S)| = 2^n$
What if S is infinite?

Theorem

Let S be a set. Then $|S| < |P(S)|$

Proof.

Define $f : S \to P(S)$ as

$$f(a) = \{a\}$$

Clearly, f is an injection. Hence $|S| \leq |P(S)|$
Claim: Any function $g : S \to P(S)$ is not surjective (hence not bijective).

$$A = \{x | x \notin g(x)\} \in P(S)$$

Suppose g is surjective.

$$A = g(a) \text{ for some } a \in S$$
$$a \in A \Leftrightarrow a \in \{x | x \notin g(x)\}$$
$$\Leftrightarrow a \notin g(a)$$
$$\Leftrightarrow a \notin A$$

Contradiction to g is surjective.

Hence $|S| \neq |P(S)|$