How ”big” can a set be?

September 18, 2011

The cardinality of sets

Question

What is the "size" of a set?

The cardinality of sets

Question

What is the "size" of a set?

Question

Can we "compare" any two sets?

The cardinality of sets

Question

What is the "size" of a set?

Question

Can we "compare" any two sets?

Observation

In this section we shall develop the tools that will enable us to compare sets. We will also prove that there "unlimited" sizes of sets and that there are many non computable functions.

Classification of functions

Definition

1. $f : A \to B$ is **one to one**, $1-1$, (injective) if $f(x) = f(y) \to x = y$

Classification of functions

Definition

1. $f : A \to B$ is **one to one**, $1-1$, (injective) if $f(x) = f(y) \to x = y$
2. $f : A \to B$ is **onto** or surjective if $\forall b \in B, \exists a \in A$ such that $f(a) = b$

Classification of functions

Definition

1. $f : A \to B$ is **one to one**, $1-1$, (injective) if $f(x) = f(y) \to x = y$
2. $f : A \to B$ is **onto** or surjective if $\forall b \in B, \exists a \in A$ such that $f(a) = b$
3. $f : A \to B$ which is both $1-1$ and onto is called a one-to-one correspondence or a **bijection**.

Classification of functions

Definition

1. $f : A \to B$ is **one to one**, $1-1$, (injective) if $f(x) = f(y) \to x = y$
2. $f : A \to B$ is **onto** or surjective if $\forall b \in B, \exists a \in A$ such that $f(a) = b$
3. $f : A \to B$ which is both $1-1$ and onto is called a one-to-one correspondence or a **bijection**.

Observation

The function $f(n) = 2n$ is a bijection between the integers and the even integers.
This means that there is a bijection between a set and "half" its size!

The inverse function

We need a few more definitions to be ready for our goal.

Definition

A set B is finite if there is a bijection between B and N_k.

Observation

If $f : A \to B$ is a bijection then we can define a new function $f^{-1} : B \to A$, the inverse of f, as follows: to find how f^{-1} maps the element $b \in B$ find the unique $a \in A$ such that: $f(a) = b$ and define $f^{-1}(b) = a$.

The inverse function

We need a few more definitions to be ready for our goal.

Definition

A set B is finite if there is a bijection between B and N_k.

Observation

If $f : A \rightarrow B$ is a bijection then we can define a new function $f^{-1} : B \rightarrow A$, the inverse of f, as follows: to find how f^{-1} maps the element $b \in B$ find the unique $a \in A$ such that: $f(a) = b$ and define $f^{-1}(b) = a$.

Example

$f(x) = 3x + 1, \; x \in R$.
$f^{-1}(x) = ?$

Definition

Let $g : A \to$B and $f : B \to C$. The **composition** of the functions f and g, denoted by $f \circ g$ is a function $f \circ g : A \to C$ defined by $f \circ g(a) = f(g(a))$.

Observation

Observation: If $f : A \to B$ *and* $g : B \to C$ *are bijections then* $g \circ f : A \to C$ *and* $f^{-1} \circ g^{-1} : C \to A$ *are also a bijections..*

Definition

Let $g : A \rightarrow$B and $f : B \rightarrow C$. The **composition** of the functions f and g, denoted by $f \circ g$ is a function $f \circ g : A \rightarrow C$ defined by $f \circ g(a) = f(g(a))$.

Observation

Observation: If $f : A \rightarrow B$ and $g : B \rightarrow C$ are bijections then $g \circ f : A \rightarrow C$ and $f^{-1} \circ g^{-1} : C \rightarrow A$ are also a bijections..

Definition

The function $f : A \rightarrow A$ defined by $f(a) = a \ \forall a \in A$ is called the **Identity** function. We denote it by I.

Definition

Let $g : A \to$B and $f : B \to C$. The **composition** of the functions f and g, denoted by $f \circ g$ is a function $f \circ g : A \to C$ defined by $f \circ g(a) = f(g(a))$.

Observation

Observation: If $f : A \to B$ and $g : B \to C$ are bijections then $g \circ f : A \to C$ and $f^{-1} \circ g^{-1} : C \to A$ are also a bijections..

Definition

The function $f : A \to A$ defined by $f(a) = a \; \forall a \in A$ is called the **Identity** function. We denote it by I.

Observation

If f is a function on the set A, then $f \circ I(a) = I \circ f(a) = f(a)$.

Example

1. Let $f(x) = \frac{x}{1+x}$ and $g(x) = \frac{x}{1+3x}$

$f \circ g(1) = f(\frac{1}{4}) =?$

Example

1. Let $f(x) = \frac{x}{1+x}$ and $g(x) = \frac{x}{1+3x}$

$f \circ g(1) = f(\frac{1}{4}) = ?$

$g \circ f(1) = g(\frac{1}{2}) = ?$

Example

1\. Let $f(x) = \frac{x}{1+x}$ and $g(x) = \frac{x}{1+3x}$

$f \circ g(1) = f(\frac{1}{4}) = ?$

$g \circ f(1) = g(\frac{1}{2}) = ?$

Coincidence???

Example

1. Let $f(x) = \frac{x}{1+x}$ and $g(x) = \frac{x}{1+3x}$

$f \circ g(1) = f(\frac{1}{4}) =?$

$g \circ f(1) = g(\frac{1}{2}) =?$

Coincidence???

2. Let $h(x) = x^2 + 1$.

$f \circ h(1) =?$ $\quad h \circ f(1) =?$.

Example

1. Let $f(x) = \frac{x}{1+x}$ and $g(x) = \frac{x}{1+3x}$
$f \circ g(1) = f(\frac{1}{4}) =?$

$g \circ f(1) = g(\frac{1}{2}) =?$

Coincidence???
2. Let $h(x) = x^2 + 1$.
$f \circ h(1) =? \qquad h \circ f(1) =?$.

$f \circ g(x)$ and $g \circ f(x)$ can be distinct functions, or the composition is not commutative.

The bijections on a set A form a group.

Theorem

If f, g, h are bijections on the set A then $(f \circ g) \circ h = f \circ (g \circ h)$

The bijections on a set A form a group.

Theorem

If f, g, h are bijections on the set A then $(f \circ g) \circ h = f \circ (g \circ h)$

Proof.

Follows easily from the definitions. $\square$

The bijections on a set A form a group.

Theorem

If f, g, h are bijections on the set A then $(f \circ g) \circ h = f \circ (g \circ h)$

Proof.

Follows easily from the definitions. □

Observation

The bijections on a set A are closed under composition, have an identity, an inverse and they are associative thus they form a group, a non-commutative group.

The bijections on a set A form a group.

Theorem

If f, g, h are bijections on the set A then $(f \circ g) \circ h = f \circ (g \circ h)$

Proof.

Follows easily from the definitions. □

Observation

The bijections on a set A are closed under composition, have an identity, an inverse and they are associative thus they form a group, a non-commutative group.

Question

You have seen compositions before, where?

The bijections on a set A form a group.

Theorem

If f, g, h are bijections on the set A then $(f \circ g) \circ h = f \circ (g \circ h)$

Proof.

Follows easily from the definitions. □

Observation

The bijections on a set A are closed under composition, have an identity, an inverse and they are associative thus they form a group, a non-commutative group.

Question

You have seen compositions before, where?

Infinities...

Definition

If there is a bijection between A and B we say that they have the same **cardinality** denoted by $\mid A \mid = \mid B \mid$

Remark

The relation $\mid A \mid = \mid B \mid$ *is an equivalence relation among sets.*

Question

1. *Naturally, we would like to say that* $\mid A \mid > \mid B \mid$ *if there is an injection* $f : B \rightarrow A$.
2. *Is this a proper comparison function? Can any two sets be compared? Can we decide which is "bigger?" Easy for finite sets, but what about infinite sets?*
3. *In particular, if* $\mid A \mid \geq \mid B \mid \wedge \mid B \mid \geq \mid A \mid$ *does it imply that* $\mid A \mid = \mid B \mid$?

Countable sets

Countable sets play a central role in discrete mathematics.

Definition

A set B is **countable** if $|B| = |N|$. We say that the cardinality of B is $\aleph_0$.

Countable sets

Countable sets play a central role in discrete mathematics.

Definition

A set B is **countable** if $\mid B \mid = \mid N \mid$. We say that the cardinality of B is $\aleph_0$.

Observation

- *If $A \subset N, \ A \neq \emptyset$ then A has a smallest member.*
- *(The axiom of mathematical induction).*
  If $1 \in A, \ \wedge \ ((n \in A) \rightarrow n+1 \in A)$ then $A = Z^+$.

Countable sets

Countable sets play a central role in discrete mathematics.

Definition

A set B is **countable** if $\mid B \mid = \mid N \mid$. We say that the cardinality of B is $\aleph_0$.

Observation

- *If $A \subset N,\ A \neq \emptyset$ then A has a smallest member.*
- *(The axiom of mathematical induction).*
  If $1 \in A,\ \wedge ((n \in A) \rightarrow n+1 \in A)$ then $A = Z^+$.

Observation

There are other equivalent forms of the principle of mathematical induction:

1. $1 \in A,\ (\forall k < n,\ k \in A \rightarrow n \in A)$ then $A = Z^+$.

2. If $(\exists a_n \in A,\ a_n \rightarrow \infty) \rightarrow (a_n - 1) \in A$ then $A = Z^+$.

Countable sets

Theorem

A subset of a countable set is either finite or countable.

Countable sets

Theorem

A subset of a countable set is either finite or countable.

Theorem

$| N \times N | = \aleph_0$.

Countable sets

Theorem

A subset of a countable set is either finite or countable.

Theorem

$| N \times N | = \aleph_0$.

Corollary

The set of rational numbers is countable ($| Q | = \aleph_0$).

Countable sets

Theorem

A subset of a countable set is either finite or countable.

Theorem

$| N \times N | = \aleph_0$.

Corollary

The set of rational numbers is countable ($| Q | = \aleph_0$).

Theorem

If $A_i, \; i = 1, 2, \ldots$ *are countable sets then so is* $\cup_{i=1}^{\infty} A_i$.

Theorem (1)

$\forall A, \mid P(A) \mid > \mid A \mid .$

Theorem (1)

$\forall A, \mid P(A) \mid > \mid A \mid$.

Theorem (2)

The set $\{x \mid 0 < x < 1, \ x \in R\}$ *is not countable.*

Theorem (1)

$\forall A, \ | P(A) | > | A |$.

Theorem (2)

The set $\{x \mid 0 < x < 1, \ x \in R\}$ *is not countable.*

Theorem (3)

The set of functions $f : N \to \{0, 1\}$ *is not countable.*

Theorem (1)

$\forall A, \mid P(A) \mid > \mid A \mid .$

Theorem (2)

The set $\{x \mid 0 < x < 1, \ x \in R\}$ *is not countable.*

Theorem (3)

The set of functions $f : N \rightarrow \{0, 1\}$ *is not countable.*

Corollary

There are functions $f : N \rightarrow \{0, 1\}$ *(decision problems) that are not programmable.*

Theorem (4)

If $\mid A \mid \leq \mid B \mid$ *and* $\mid B \mid \leq \mid A \mid$ *then* $\mid A \mid = \mid B \mid$

Proofs

Here are some brief hints for the proofs.

Proofs

Here are some brief hints for the proofs.

Proof (Sketch of a proof for theorem 1)

We will prove that there is no onto function $f : A \to P(A)$ *.*
Indeed given any function $f : A \to P(A)$*. Let* $S = \{a \in A \mid a \notin f(a)\}$*.*
(Recall that $f(a) \subset A$*, or* $f(a) \in P(A)$*).*

Proofs

Here are some brief hints for the proofs.

Proof (Sketch of a proof for theorem 1)

We will prove that there is no onto function $f : A \to P(A)$ *.*
Indeed given any function $f : A \to P(A)$*. Let* $S = \{a \in A \mid a \notin f(a)\}$*.*
(Recall that $f(a) \subset A$*, or* $f(a) \in P(A)$*).*
Assume that $S = f(s)$ *for some* $s \in A$*.*
Whether $s \in f(s)$ *or* $s \notin f(s)$ *we reach a contradicion.*

Proofs

Here are some brief hints for the proofs.

Proof (Sketch of a proof for theorem 1)

We will prove that there is no onto function $f : A \to P(A)$ *.*
Indeed given any function $f : A \to P(A)$*. Let* $S = \{a \in A \mid a \notin f(a)\}$*.*
(Recall that $f(a) \subset A$*, or* $f(a) \in P(A)$*).*
Assume that $S = f(s)$ *for some* $s \in A$*.*
Whether $s \in f(s)$ *or* $s \notin f(s)$ *we reach a contradicion.*
Fill in the details.
Conclusion: since there is an injection $g : A \to P(A)$ *and there is no onto function* $f : A \to P(A)$ *we conclude that* $\mid A \mid < \mid P(A) \mid$*.*

Proofs

Proof (Sketch of a proof for theorem 2)

For every countable set $A \subset \{x \mid 0 < x < 1,\ x \in R\} = \mathbb{U}$ *we shall find a real number* $y \notin A$.

Proofs

Proof (Sketch of a proof for theorem 2)

For every countable set $A \subset \{x \mid 0 < x < 1,\ x \in R\} = \mathbb{U}$ *we shall find a real number* $y \notin A$.
Let $\{x_1, x_2, \ldots, x_n, \ldots\}$ *be a countable subset of* $\mathbb{U}$. *Let* $x_n = 0.x_{n,1}x_{n,2}\ldots x_{n,n}x_{n,n+1}\ldots$ *be the decimal expansion of* x_n.

Proof (Sketch of a proof for theorem 2)

For every countable set $A \subset \{x \mid 0 < x < 1,\ x \in R\} = \mathbb{U}$ *we shall find a real number* $y \notin A$.
Let $\{x_1, x_2, \ldots, x_n, \ldots\}$ *be a countable subset of* $\mathbb{U}$. *Let* $x_n = 0.x_{n,1}x_{n,2}\ldots x_{n,n}x_{n,n+1}\ldots$ *be the decimal expansion of* x_n.

Let $y = 0.y_1y_2\ldots y_n\ldots$ *be defined as follows:*

Let $y_n = x_{n,n} + 5 \pmod{10}$. *We want to make sure that* $\forall n,\ y_n \neq x_{n,n}$.

Proofs

Proof (Sketch of a proof for theorem 2)

For every countable set $A \subset \{x \mid 0 < x < 1,\ x \in R\} = \mathbb{U}$ *we shall find a real number* $y \notin A$.
Let $\{x_1, x_2, \ldots, x_n, \ldots\}$ *be a countable subset of* $\mathbb{U}$. *Let* $x_n = 0.x_{n,1}x_{n,2}\ldots x_{n,n}x_{n,n+1}\ldots$ *be the decimal expansion of* x_n.

Let $y = 0.y_1y_2\ldots y_n\ldots$ *be defined as follows:*

Let $y_n = x_{n,n} + 5 \pmod{10}$. *We want to make sure that* $\forall n,\ y_n \neq x_{n,n}$.

Fill in the details, that is prove that $y \notin A$.

Proofs

Proof (Sketch of a proof for theorem 2)

For every countable set $A \subset \{x \mid 0 < x < 1,\ x \in R\} = \mathbb{U}$ *we shall find a real number* $y \notin A$.
Let $\{x_1, x_2, \ldots, x_n, \ldots\}$ *be a countable subset of* $\mathbb{U}$. *Let* $x_n = 0.x_{n,1}x_{n,2}\ldots x_{n,n}x_{n,n+1}\ldots$ *be the decimal expansion of* x_n.

Let $y = 0.y_1y_2\ldots y_n\ldots$ *be defined as follows:*

Let $y_n = x_{n,n} + 5 \pmod{10}$. *We want to make sure that* $\forall n,\ y_n \neq x_{n,n}$.

Fill in the details, that is prove that $y \notin A$.

Remark

This proof technique is called the Diagonal Method. It is used on many occaisons. For instance Theorem 1 is an abstract form of this method.

Proofs

Here we go again.

Proof (Theorem 3, proof sketch)

It is enough to show that there is a bijection between the set of functions: $\{f : N \to \{0, 1\}\}$ *and* $P(N)$.

Proofs

Here we go again.

Proof (Theorem 3, proof sketch)

It is enough to show that there is a bijection between the set of functions: $\{f : N \to \{0, 1\}\}$ *and* $P(N)$.
Let $F(f) = \{i \mid f(i) = 1\}$.
Show that this is a bijection between $P(n)$ *and the functions.*

Proofs

Here we go again.

Proof (Theorem 3, proof sketch)

It is enough to show that there is a bijection between the set of functions:
$\{f : N \to \{0, 1\}\}$ *and* $P(N)$.
Let $F(f) = \{i \mid f(i) = 1\}$.
Show that this is a bijection between $P(n)$ *and the functions.*

Proof (of the corollary)

Each program that implements a decision problem is stored in memory as a finite binary sequence. There are only countably many finite binary sequences. Hence there are non computable functions.

Proofs

Proof (of theorem 4)

The theorem says that if there are $1-1$ *functions* $f : A \to B$ and $g : B \to A$ *then there is a bijection between* A and B.

Proofs

Proof (of theorem 4)

The theorem says that if there are $1-1$ *functions* $f : A \to B$ and $g : B \to A$ *then there is a bijection between* A and B.

Consider the following chains, (directed paths): $\ldots \to a \to f(a) \to g(f(a) \ldots$

Proof (of theorem 4)

The theorem says that if there are $1-1$ *functions* $f : A \rightarrow B$ and $g : B \rightarrow A$ *then there is a bijection between* A and B.

Consider the following chains, (directed paths): $\ldots \rightarrow a \rightarrow f(a) \rightarrow g(f(a) \ldots$
Verify: Each chain is one of the following four types:

1. *A finite cycle with* $2n$ *"nodes"* n*, members of* A *interlaced with* n *members of .*

Proofs

Proof (of theorem 4)

The theorem says that if there are $1-1$ *functions* $f : A \to B$ *and* $g : B \to A$ *then there is a bijection between* A *and* B.

Consider the following chains, (directed paths): $\ldots \to a \to f(a) \to g(f(a) \ldots$

Verify: Each chain is one of the following four types:

1. *A finite cycle with 2n "nodes" n, members of A interlaced with n members of .*
2. *A doubly infinite chain of interlaced nodes from A and B.*

Proof (of theorem 4)

The theorem says that if there are $1-1$ *functions* $f: A \to B$ and $g: B \to A$ *then there is a bijection between* A and B.

Consider the following chains, (directed paths): $\ldots \to a \to f(a) \to g(f(a) \ldots$

Verify: Each chain is one of the following four types:

1. *A finite cycle with* $2n$ *"nodes"* n*, members of* A *interlaced with* n *members of .*
2. *A doubly infinite chain of interlaced nodes from* A *and* B.
3. *An infinite chain* $a \to b \to a' \to b' \to \ldots$

Proofs

Proof (of theorem 4)

The theorem says that if there are $1-1$ *functions* $f : A \to B$ and $g : B \to A$ *then there is a bijection between* A and B.

Consider the following chains, (directed paths): $\ldots \to a \to f(a) \to g(f(a) \ldots$
Verify: Each chain is one of the following four types:

1. *A finite cycle with* $2n$ *"nodes"* n*, members of* A *interlaced with* n *members of .*
2. *A doubly infinite chain of interlaced nodes from* A *and* B*.*
3. *An infinite chain* $a \to b \to a' \to b' \to \ldots$
4. *An infinite chain* $b \to a \to b' \to a' \to \ldots$

Proof of theorem 4, continued

We note that each $a \in A, \; and \; b \in B$ is included in exactly one chain.

Proof of theorem 4, continued

We note that each $a \in A,\ and\ b \in B$ is included in exactly one chain.
Each $a \in A$ has a succsessor in B

Proof of theorem 4, continued

We note that each $a \in A,\ and\ b \in B$ is included in exactly one chain.
Each $a \in A$ has a succsessor in B
Each $a \in A$ has a predecessor in B except for the head of the chains in (3).

Proof of theorem 4, continued

We note that each $a \in A,$ *and* $b \in B$ is included in exactly one chain.
Each $a \in A$ has a succsessor in B
Each $a \in A$ has a predecessor in B except for the head of the chains in (3).
Each $b \in B$ has a successor in A.

Proof of theorem 4, continued

We note that each $a \in A,$ *and* $b \in B$ is included in exactly one chain.
Each $a \in A$ has a succsessor in B
Each $a \in A$ has a predecessor in B except for the head of the chains in (3).
Each $b \in B$ has a successor in A.
Each $b \in B$ has a predecessor in A except for the head of the chains in (4).

Proof of theorem 4, continued

We note that each $a \in A, \ and \ b \in B$ is included in exactly one chain.
Each $a \in A$ has a succsessor in B
Each $a \in A$ has a predecessor in B except for the head of the chains in (3).
Each $b \in B$ has a successor in A.
Each $b \in B$ has a predecessor in A except for the head of the chains in (4).
The mapping $F(a) = b$ where $a \to b$, if a belongs to chains in (1), (2) or (3) and $F(a) = b$ where $b \to a$ if a is in a chain of (4) is a bijection between A and B.

Proof of theorem 4, continued

We note that each $a \in A,$ *and* $b \in B$ is included in exactly one chain.
Each $a \in A$ has a succsessor in B
Each $a \in A$ has a predecessor in B except for the head of the chains in (3).
Each $b \in B$ has a successor in A.
Each $b \in B$ has a predecessor in A except for the head of the chains in (4).
The mapping $F(a) = b$ where $a \to b$, if a belongs to chains in (1), (2) or (3) and $F(a) = b$ where $b \to a$ if a is in a chain of (4) is a bijection between A and B.
Verify this assertion.

In Set Theory this is known as bernstein's Lemma.

Surprise

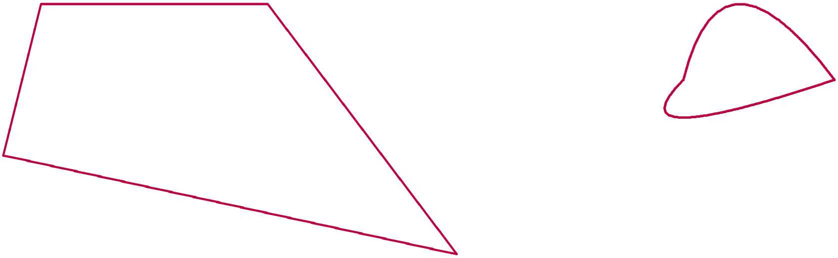
Remark

There is a surprising consequence of this famous lemma. If you take two sets of points A and B in the plane, and if each set contains a disk, then each set can be disected into two sets A_1, A_2, B_1, B_2 such that A_i and B_i are similar.

Surprise

Remark

There is a surprising consequence of this famous lemma. If you take two sets of points A and B in the plane, and if each set contains a disk, then each set can be disected into two sets A_1, A_2, B_1, B_2 such that A_i and B_i are similar.



For example: these two sets can be disected into a pair of similar sets!