CS 207 Discrete Mathematics – 2012-2013

Nutan Limaye

Indian Institute of Technology, Bombay
nutan@cse.iitb.ac.in

Mathematical Reasoning and Mathematical Objects

Lecture 3: Mathematical structures

Aug 01, 2012

Last time

Recap

- The principle of induction: we proved that $\forall i, j \in \mathbb{N},\ f(i,j) < i+1$, where $f(i,j) = \sqrt{i\sqrt{i+1 \ldots \sqrt{j-1\sqrt{j}}}}$.

Recap

- The principle of induction: we proved that $\forall i, j \in \mathbb{N},\ f(i,j) < i+1$, where $f(i,j) = \sqrt{i\sqrt{i+1 \ldots \sqrt{j-1\sqrt{j}}}}$.
- Take back message: be careful when proving statements by induction.

Mathematical Structures

sets, functions, relations, graphs ...

What are sets?

A set can be vaguely defined as a collection of objects.

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

The barber's dilema

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

The barber's dilema
Once upon a time there was a kingdom in which the king ordered the barber to shave only those who do not shave themselves!

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

The barber's dilema
Once upon a time there was a kingdom in which the king ordered the barber to shave only those who do not shave themselves!
Of course, barber could neither shave himself and nor could he not shave himself!

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

The barber's dilema
Once upon a time there was a kingdom in which the king ordered the barber to shave only those who do not shave themselves!
Of course, barber could neither shave himself and nor could he not shave himself!
This is called a paradox.

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

Cantor was the first person to define sets formally – finite sets as well as infinite sets, and prove important properties related to sets.
Let P be a property then he said any collection of objects which satisfy property P is a set, i.e.
$S = \{x \mid P(x)\}$.

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

Cantor was the first person to define sets formally – finite sets as well as infinite sets, and prove important properties related to sets.
Let P be a property then he said any collection of objects which satisfy property P is a set, i.e.
$S = \{x \mid P(x)\}$.

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

Russell's paradox:
$A = \{X \mid X \notin X\}$
Now if $A \in A$ then $A \notin A$ and if $A \notin A$ then $A \in A$!

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

Russell's paradox:
$A = \{X \mid X \notin X\}$
Now if $A \in A$ then $A \notin A$ and if $A \notin A$ then $A \in A$!

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

(CW) Can you come up with a set that contains itself?

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

How to get around this paradox?

Definition

Start with a few objects *defined* as sets. Now if A is a set and P is a property, then $S = \{x \in A \mid P(x)\}$ is also a set.

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

How to get around this paradox?

Definition

Start with a few objects *defined* as sets. Now if A is a set and P is a property, then $S = \{x \in A \mid P(x)\}$ is also a set.

Why does this definition get rid of Russell's paradox?

- Let $P(x) = x \notin x$. Suppose A is a set and let $S = \{x \in A \mid x \notin x\}$.

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

How to get around this paradox?

Definition

Start with a few objects *defined* as sets. Now if A is a set and P is a property, then $S = \{x \in A \mid P(x)\}$ is also a set.

Why does this definition get rid of Russell's paradox?

- Let $P(x) = x \notin x$. Suppose A is a set and let $S = \{x \in A \mid x \notin x\}$.
  - ($S \in S$:) from the definition of S, $S \in A$ and $S \notin S$, which is a contradiction.
  - ($S \notin S$:) from the definition, either $S \notin A$ or $S \in S$. But we have assumed that $S \notin S$, therefore it must mean $S \notin A$. There is no contradiction!

What are sets?

A set can be vaguely defined as a collection of objects.
But vague definitions can lead to problems.

How to get around this paradox?

Definition

Start with a few objects *defined* as sets. Now if A is a set and P is a property, then $S = \{x \in A \mid P(x)\}$ is also a set.

Why does this definition get rid of Russell's paradox?

- Let $P(x) = x \notin x$. Suppose A is a set and let $S = \{x \in A \mid x \notin x\}$.
  - ($S \in S$:) from the definition of S, $S \in A$ and $S \notin S$, which is a contradiction.
  - ($S \notin S$:) from the definition, either $S \notin A$ or $S \in S$. But we have assumed that $S \notin S$, therefore it must mean $S \notin A$. There is no contradiction!

How to get around Barber's paradox? (CW)

Examples and properties

- We have already seen sets such as $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ etc.

Examples and properties

- We have already seen sets such as $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ etc.
- Let A, B be two sets. Their cartesian product, $A \times B$, is defined as $A \times B = \{(a, b) \mid a \in A, b \in B\}$
- Similarly, union, intersection, symmetric difference are defined as:
  $A \cup B = \{x \mid a \in A \text{ or } x \in B\}$
  $A \cap B = \{x \mid a \in A \text{ and } x \in B\}$
  $A \oplus B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$

Examples and properties

- We have already seen sets such as $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ etc.
- Let A, B be two sets. Their cartesian product, $A \times B$, is defined as $A \times B = \{(a, b) \mid a \in A, b \in B\}$
- Similarly, union, intersection, symmetric difference are defined as:
  $A \cup B = \{x \mid a \in A \text{ or } x \in B\}$
  $A \cap B = \{x \mid a \in A \text{ and } x \in B\}$
  $A \oplus B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$
  $\wedge$: and
  $\vee$: or

Examples and properties

- We have already seen sets such as $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ etc.
- Let A, B be two sets. Their cartesian product, $A \times B$, is defined as $A \times B = \{(a, b) \mid a \in A, b \in B\}$
- Similarly, union, intersection, symmetric difference are defined as:
  $A \cup B = \{x \mid a \in A \text{ or } x \in B\}$
  $A \cap B = \{x \mid a \in A \text{ and } x \in B\}$
  $A \oplus B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$
- Let U be the universe. The complement of a set A with respect to the universe U, denoted as $\bar{A}$ or $A^c = \{x \in U \mid x \notin A\}$.

Examples and properties

- We have already seen sets such as $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ etc.
- Let A, B be two sets. Their cartesian product, $A \times B$, is defined as $A \times B = \{(a, b) \mid a \in A, b \in B\}$
- Similarly, union, intersection, symmetric difference are defined as:
  $A \cup B = \{x \mid a \in A \text{ or } x \in B\}$
  $A \cap B = \{x \mid a \in A \text{ and } x \in B\}$
  $A \oplus B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$
- Let U be the universe. The complement of a set A with respect to the universe U, denoted as $\bar{A}$ or $A^c = \{x \in U \mid x \notin A\}$.
- The powerset, $\mathcal{P}(A)$, of a set A is defined to be a collection of all subsets of A.

Examples and properties

- We have already seen sets such as $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ etc.
- Let A, B be two sets. Their cartesian product, $A \times B$, is defined as $A \times B = \{(a, b) \mid a \in A, b \in B\}$
- Similarly, union, intersection, symmetric difference are defined as:
  $A \cup B = \{x \mid a \in A \text{ or } x \in B\}$
  $A \cap B = \{x \mid a \in A \text{ and } x \in B\}$
  $A \oplus B = \{x \mid (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$
- Let U be the universe. The complement of a set A with respect to the universe U, denoted as $\bar{A}$ or $A^c = \{x \in U \mid x \notin A\}$.
- The powerset, $\mathcal{P}(A)$, of a set A is defined to be a collection of all subsets of A.
  Example: Let $A = \{a, b\}$ then $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Infinite sets

- We have already seen infinite sets:
  Examples: $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}$.

Infinite sets

- We have already seen infinite sets:
  Examples: $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}$.
- How do we measure the size of any set? For a set S, finite or infinite, $|S|$ denotes the size of that set. It is also called the *cardinality* of the set.

Infinite sets

- We have already seen infinite sets:
  Examples: $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}$.
- How do we measure the size of any set? For a set S, finite or infinite, $|S|$ denotes the size of that set. It is also called the *cardinality* of the set.
- For a finite set, $|S|$ equals the number of elements in S.

Infinite sets

- We have already seen infinite sets:
  Examples: $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}$.
- How do we measure the size of any set? For a set S, finite or infinite, $|S|$ denotes the size of that set. It is also called the *cardinality* of the set.
- For a finite set, $|S|$ equals the number of elements in S.
- What about infinite sets?

Infinite sets

- We have already seen infinite sets:
  Examples: $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}$.
- How do we measure the size of any set? For a set S, finite or infinite, $|S|$ denotes the size of that set. It is also called the *cardinality* of the set.
- For a finite set, $|S|$ equals the number of elements in S.
- What about infinite sets?
- Given two infinite sets, can we talk about one being *bigger* than the other? If so, how?

Functions

Definition

Let A, B be two sets. A function from A to B, $f : A \to B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional property that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

Functions

Definition

Let A, B be two sets. A function from A to B, $f : A \to B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional property that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

- Here, b is called an image of a, denoted as $f(a) = b$.

Functions

Definition

Let A, B be two sets. A function from A to B, $f : A \to B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional property that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

- Here, b is called an image of a, denoted as $f(a) = b$.
- $Range(f) = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\}$

Functions

Definition

Let A, B be two sets. A function from A to B, $f : A \rightarrow B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional property that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

- Here, b is called an image of a, denoted as $f(a) = b$.
- $Range(f) = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\} \subseteq B$

Functions

Definition

Let A, B be two sets. A function from A to B, $f : A \to B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional property that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

- Here, b is called an image of a, denoted as $f(a) = b$.
- $Range(f) = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\} \subseteq B$
  $\subseteq$: Subset of

Functions

Definition

Let A, B be two sets. A function from A to B, $f : A \rightarrow B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional property that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

- Here, b is called an image of a, denoted as $f(a) = b$.
- $Range(f) = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\} \subseteq B$
- $Domain(f) = A$

Functions

Definition

Let A, B be two sets. A function from A to B, $f : A \to B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional property that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.

- Here, b is called an image of a, denoted as $f(a) = b$.
- $Range(f) = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\} \subseteq B$
- $Domain(f) = A$

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n + 1$ injective?

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n + 1$ injective?
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n^2$ injective?

Types of functions

- Injective function, one-to-one: A function $f : A \rightarrow B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
  - Is $f : \mathbb{Z} \rightarrow \mathbb{Z}$, defined as $f(n) = n + 1$ injective?
  - Is $f : \mathbb{Z} \rightarrow \mathbb{Z}$, defined as $f(n) = n^2$ injective?
  - What about $f : \mathbb{Z} \rightarrow \mathbb{Z}$, defined as $f(n) = \sqrt{n}$?

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \to B$ is said to be surjective if $\forall x \in B\ \exists a \in A$ such that $f(a) = x$.
- Bijective function: A function is said to be bijective if it is surjective and injective.

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \to B$ is said to be surjective if $\forall x \in B\ \exists a \in A$ such that $f(a) = x$.
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n + 1$ surjective?
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n^2$ surjective?
  - What about $f : \mathbb{R} \to \mathbb{R}$, defined as $f(x) = 10x - 7$?

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \to B$ is said to be surjective if $\forall x \in B\ \exists a \in A$ such that $f(a) = x$.
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n + 1$ surjective?
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n^2$ surjective?
  - What about $f : \mathbb{R} \to \mathbb{R}$, defined as $f(x) = 10x - 7$?

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \to B$ is said to be surjective if $\forall x \in B\ \exists a \in A$ such that $f(a) = x$.
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n + 1$ surjective?
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n^2$ surjective?
  - What about $f : \mathbb{R} \to \mathbb{R}$, defined as $f(x) = 10x - 7$?
- Bijective function: A function is said to be bijective if it is surjective and injective.

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \to B$ is said to be surjective if $\forall x \in B\ \exists a \in A$ such that $f(a) = x$.
- Bijective function: A function is said to be bijective if it is surjective and injective.

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \to B$ is said to be surjective if $\forall x \in B\ \exists a \in A$ such that $f(a) = x$.
- Bijective function: A function is said to be bijective if it is surjective and injective.
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n + 1$ bijective?
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n^2$ bijective?
  - What about $f : \mathbb{R} \to \mathbb{R}$, defined as $f(x) = 10x - 7$?

Types of functions

- Injective function, one-to-one: A function $f : A \rightarrow B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \rightarrow B$ is said to be surjective if $\forall x \in B\ \exists a \in A$ such that $f(a) = x$.
- Bijective function: A function is said to be bijective if it is surjective and injective.
  - Is $f : \mathbb{Z} \rightarrow \mathbb{Z}$, defined as $f(n) = n + 1$ bijective?
  - Is $f : \mathbb{Z} \rightarrow \mathbb{Z}$, defined as $f(n) = n^2$ bijective?
  - What about $f : \mathbb{R} \rightarrow \mathbb{R}$, defined as $f(x) = 10x - 7$?

Types of functions

- Injective function, one-to-one: A function $f : A \to B$ is said to be injective if $\forall x, y \in A$ if $f(x) = f(y)$ then $x = y$.
- Surjective function, onto: A function $f : A \to B$ is said to be surjective if $\forall x \in B$ $\exists a \in A$ such that $f(a) = x$.
- Bijective function: A function is said to be bijective if it is surjective and injective.
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n + 1$ bijective?
  - Is $f : \mathbb{Z} \to \mathbb{Z}$, defined as $f(n) = n^2$ bijective?
  - What about $f : \mathbb{R} \to \mathbb{R}$, defined as $f(x) = 10x - 7$?

Back to infinite sets

We will understand the notion of *size of an infinite set* in a relative sense.

Definition

We say that two sets A, B have the same size if and only if there is a bijection between A and B

Back to infinite sets

We will understand the notion of *size of an infinite set* in a relative sense.

Definition

We say that two sets A, B have the same size if and only if there is a bijection between A and B

Examples

- Let E be a set of even numbers. There is a bijection between E and $\mathbb{N}$

Back to infinite sets

We will understand the notion of *size of an infinite set* in a relative sense.

Definition

We say that two sets A, B have the same size if and only if there is a bijection between A and B

Examples

- Let E be a set of even numbers. There is a bijection between E and $\mathbb{N}$ $f(x) = 2x, f : \mathbb{N} \to E$.

Back to infinite sets

We will understand the notion of *size of an infinite set* in a relative sense.

Definition

We say that two sets A, B have the same size if and only if there is a bijection between A and B

Examples

- Let E be a set of even numbers. There is a bijection between E and $\mathbb{N}$
- There is a bijection $f : \mathbb{Z} \to \mathbb{N}$

Back to infinite sets

We will understand the notion of *size of an infinite set* in a relative sense.

Definition

We say that two sets A, B have the same size if and only if there is a bijection between A and B

Examples

- Let E be a set of even numbers. There is a bijection between E and $\mathbb{N}$
- There is a bijection $f : \mathbb{Z} \rightarrow \mathbb{N}$

$$f(x) = \begin{cases} -2x & \text{if } x \leq 0 \\ 2x - 1 & \text{otherwise} \end{cases}$$

Back to infinite sets

We will understand the notion of *size of an infinite set* in a relative sense.

Definition

We say that two sets A, B have the same size if and only if there is a bijection between A and B

Examples

- Let E be a set of even numbers. There is a bijection between E and $\mathbb{N}$
- There is a bijection $f : \mathbb{Z} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Back to infinite sets

We will understand the notion of *size of an infinite set* in a relative sense.

Definition

We say that two sets A, B have the same size if and only if there is a bijection between A and B

Examples

- Let E be a set of even numbers. There is a bijection between E and $\mathbb{N}$
- There is a bijection $f : \mathbb{Z} \rightarrow \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$