CS 207: Discrete Structures

Instructor : S. Akshay

July 27, 2015

Lecture 04 – Basic Mathematical Structures

Logistics

Tutorial timings

Tuesdays 5.15pm at SIC 301 Kresit building.

Recap of last three lectures

Chapter 1: Mathematical reasoning

- Propositions, predicates.
- Axioms, Theorems and Types of proofs: contradiction, contrapositive, etc.
- Principle of Mathematical Induction
- Well-ordering principle and Strong Induction

Recap of last three lectures

Chapter 1: Mathematical reasoning

- Propositions, predicates.
- Axioms, Theorems and Types of proofs: contradiction, contrapositive, etc.
- Principle of Mathematical Induction
- Well-ordering principle and Strong Induction

Today:- Chapter 2: Basic Mathematical Structures

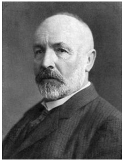
- Finite and infinite sets, Functions
- Relations

Sets

What is a set?

- A set is an unordered collection of objects.
- The objects in a set are called its elements.

Sets



§ I

The Conception of Power or Cardinal Number

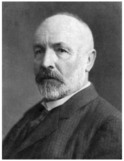
By an "aggregate" (*Menge*) we are to understand any collection into a whole (*Zusammenfassung zu einem Ganzen*) M of definite and separate objects *m* of our intuition or our thought. These objects are called the "elements" of M.

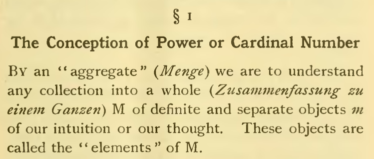
Figure : Georg Cantor (1845-1918); extract

What is a set?

- A set is an unordered collection of objects.
- The objects in a set are called its elements.

Sets





§ I

The Conception of Power or Cardinal Number

By an "aggregate" (*Menge*) we are to understand any collection into a whole (*Zusammenfassung zu einem Ganzen*) M of definite and separate objects *m* of our intuition or our thought. These objects are called the "elements" of M.

Figure : Georg Cantor (1845-1918); extract

What is a set?

- A **set** is an unordered collection of objects.
- The objects in a set are called its **elements**.

More formally,

Let P be a property. Any collection of objects that are defined by (or satisfy) P is a set, i.e., $S = \{x \mid P(x)\}$.

Some simple boring stuff about sets

Examples and properties

- We have already seen examples: $\mathbb{Z}, \mathbb{N}, \mathbb{R}$, set of all horses,...
- Let A, B be two sets. Recall the usual definitions:
  - Equality $A = B$, Subset $A \subseteq B$,
  - Cartesian product $A \times B = \{(a, b) \mid a \in A, b \in B\}$
  - Union $A \cup B = \{x \mid a \in A \text{ or } b \in B\}$
  - Intersection $A \cap B = \{x \mid a \in A \text{ and } b \in B\}$
  - Empty set ϕ,
  - Power set of $A = \mathcal{P}(A)=$ set of all subsets of A.
  - If U is the universe, then the complement of A, $\bar{A} = A^c = \{x \in U \mid x \notin A\}$.

Some simple boring stuff about sets

Examples and properties

- We have already seen examples: $\mathbb{Z}, \mathbb{N}, \mathbb{R}$, set of all horses,...
- Let A, B be two sets. Recall the usual definitions:
  - Equality $A = B$, Subset $A \subseteq B$,
  - Cartesian product $A \times B = \{(a, b) \mid a \in A, b \in B\}$
  - Union $A \cup B = \{x \mid a \in A \text{ or } b \in B\}$
  - Intersection $A \cap B = \{x \mid a \in A \text{ and } b \in B\}$
  - Empty set ϕ,
  - Power set of $A = \mathcal{P}(A)$= set of all subsets of A.
  - If U is the universe, then the complement of A, $\bar{A} = A^c = \{x \in U \mid x \notin A\}$.

So, what is the difference between $\{\emptyset\}$ and $\emptyset$?

Not so simple...

A barber is a man in town who only shaves those who don't shave themselves.

Barber's paradox: Does the barber shave himself?

Not so simple...

A barber is a man in town who only shaves those who don't shave themselves.

Barber's paradox: Does the barber shave himself?

Russell's paradox

Let $S = \{X \mid X \notin X\}$

Then if $S \in S$, then $S \notin S$ and if $S \notin S$, then $S \in S$!

Not so simple...

A barber is a man in town who only shaves those who don't shave themselves.

Barber's paradox: Does the barber shave himself?

Russell's paradox

Let $S = \{X \mid X \notin X\}$

Then if $S \in S$, then $S \notin S$ and if $S \notin S$, then $S \in S$!

How do you resolve this?

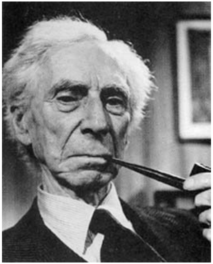


Figure : Bertrand Russell (1872-1970)

Not so simple...

A barber is a man in town who only shaves those who don't shave themselves.

Barber's paradox: Does the barber shave himself?

Russell's paradox

Let $S = \{X \mid X \notin X\}$

Then if $S \in S$, then $S \notin S$ and if $S \notin S$, then $S \in S$!

Axiomatic approach to set theory (ZFC!)

Start with a few objects defined. Then for a set A and a property P, $S = \{x \in A \mid P(x)\}$ is a set.

Not so simple...

A barber is a man in town who only shaves those who don't shave themselves.
Barber's paradox: Does the barber shave himself?

Russell's paradox

Let $S = \{X \mid X \notin X\}$
Then if $S \in S$, then $S \notin S$ and if $S \notin S$, then $S \in S$!

Axiomatic approach to set theory (ZFC!)

Start with a few objects defined. Then for a set A and a property P, $S = \{x \in A \mid P(x)\}$ is a set.

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

Not so simple...

A barber is a man in town who only shaves those who don't shave themselves.

Barber's paradox: Does the barber shave himself?

Russell's paradox

Let $S = \{X \mid X \notin X\}$
Then if $S \in S$, then $S \notin S$ and if $S \notin S$, then $S \in S$!

Axiomatic approach to set theory (ZFC!)

Start with a few objects defined. Then for a set A and a property P, $S = \{x \in A \mid P(x)\}$ is a set.

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

- if $(S \in S)$: from the definition of S, $S \in A$ and $S \notin S$, which is a contradiction.
- if $(S \notin S)$: from the definition, either $S \notin A$ or $S \in S$. But we have assumed that $S \notin S$. Hence, $S \notin A$. No contradiction!

Is the fun done? How do we compare sets?

- For two finite sets, this is easy, just count the number of elements and compare them!

Is the fun done? How do we compare sets?

- For two finite sets, this is easy, just count the number of elements and compare them!
- But what about two infinite sets?
- Example: {set of all even natural numbers} vs $\mathbb{N}$ vs $\mathbb{Q}$ vs $\mathbb{R}$

Is the fun done? How do we compare sets?

- For two finite sets, this is easy, just count the number of elements and compare them!
- But what about two infinite sets?
- Example: $\{$set of all even natural numbers$\}$ vs $\mathbb{N}$ vs $\mathbb{Q}$ vs $\mathbb{R}$
- Turns out we need functions... but first...

Hilbert's hotel

- Suppose there is a hotel with infinitely many rooms.
- And suppose they are all full (like in IIT guest house).

Hilbert's hotel

- Suppose there is a hotel with infinitely many rooms.
- And suppose they are all full (like in IIT guest house).

1. Can you accomodate 1 or finitely many more guests, by shifting around the existing guests?

Hilbert's hotel

- Suppose there is a hotel with infinitely many rooms.
- And suppose they are all full (like in IIT guest house).

1. Can you accomodate 1 or finitely many more guests, by shifting around the existing guests?
2. What if infinitely many more guests arrive?

Hilbert's hotel

- Suppose there is a hotel with infinitely many rooms.
- And suppose they are all full (like in IIT guest house).

1. Can you accomodate 1 or finitely many more guests, by shifting around the existing guests?
2. What if infinitely many more guests arrive?
3. What if infinitely many more trains with infinitely many more guests arrive? (H.W)

Functions

What you did above was to define functions...

Definition

Let A, B be two sets. A function f from A to B is an assignment of exactly one element of B to each element of A.

Functions

What you did above was to define functions...

Definition

Let A, B be two sets. A function f from A to B is an assignment of exactly one element of B to each element of A.

i.e., $f : A \to B$ is a subset R of $A \times B$ such that

(i) $\forall a \in A$, $\exists b \in B$ such that $(a, b) \in R$, and

(ii) if $(a, b) \in R$ and $(a, c) \in R$, then $b = c$.

Functions

What you did above was to define functions...

Definition

Let A, B be two sets. A function f from A to B is an assignment of exactly one element of B to each element of A.

i.e., $f : A \to B$ is a subset R of $A \times B$ such that

(i) $\forall a \in A$, $\exists b \in B$ such that $(a, b) \in R$, and

(ii) if $(a, b) \in R$ and $(a, c) \in R$, then $b = c$.

- We write $f(a) = b$ and call b the image of a.
- $Range(f) = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\}$, $Domain(f) = A$

Functions

What you did above was to define functions...

Definition

Let A, B be two sets. A function f from A to B is an assignment of exactly one element of B to each element of A.

i.e., $f : A \to B$ is a subset R of $A \times B$ such that

(i) $\forall a \in A, \exists b \in B$ such that $(a, b) \in R$, and

(ii) if $(a, b) \in R$ and $(a, c) \in R$, then $b = c$.

Composition of functions

- If $g : A \to B$ and $f : B \to C$, then $f \circ g : A \to C$ is defined by $f \circ g(x) = f(g(x))$.

- Defined only if $Range(g) \subseteq Domain(f)$.
- Example: if $f(x) = x^2$, $g(x) = x - x^3$ with $f, g : \mathbb{R} \to \mathbb{R}$, what is $f \circ g(x), g \circ f(x)$?

Functions

What you did above was to define functions...

Definition

Let A, B be two sets. A function f from A to B is an assignment of exactly one element of B to each element of A.

i.e., $f : A \to B$ is a subset R of $A \times B$ such that

(i) $\forall a \in A$, $\exists b \in B$ such that $(a, b) \in R$, and

(ii) if $(a, b) \in R$ and $(a, c) \in R$, then $b = c$.

Composition of functions is associative

- If $h : A \to B$ and $g : B \to C$ and $f : C \to D$, then $f \circ (g \circ h) = (f \circ g) \circ h$.

Check it! (H.W.)

Functions

What you did above was to define functions...

Definition

Let A, B be two sets. A function f from A to B is an assignment of exactly one element of B to each element of A.

i.e., $f : A \to B$ is a subset R of $A \times B$ such that

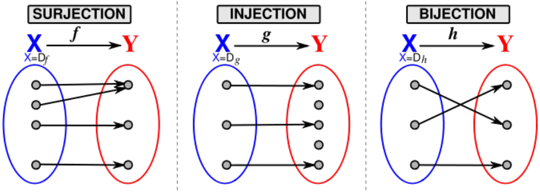
(i) $\forall a \in A, \exists b \in B$ such that $(a, b) \in R$, and

(ii) if $(a, b) \in R$ and $(a, c) \in R$, then $b = c$.

Inverse of a function

- If $f : A \to B$ is a ??? function, then $f^{-1} : B \to A$ defined by $f^{-1}(b) = a$ if $f(a) = b$, is called its inverse.

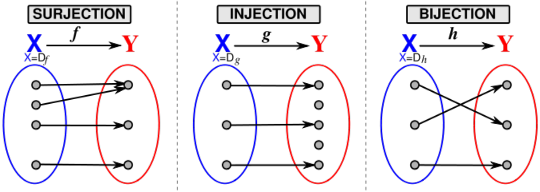
Comparing (finite and infinite) sets



- Surjective or onto: $f : A \to B$ is surjective if $\forall y \in B$, $\exists x \in A$ such that $f(x) = y$.
- Injective or 1-1: $f : A \to B$ is injective if $\forall x, y \in A$, if $f(x) = f(y)$, then $x = y$.
- Bijective or 1-1 correspondence: A function is bijective if it is surjective and injective.

If f is a bijection, then its inverse function exists and $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$

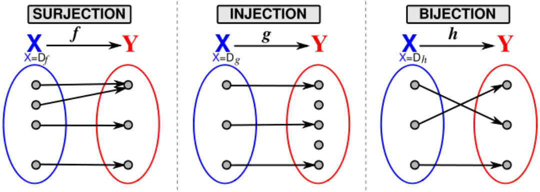
Comparing (finite and infinite) sets



- Surjective or onto: $f : A \to B$ is surjective if $\forall y \in B$, $\exists x \in A$ such that $f(x) = y$.
- Injective or 1-1: $f : A \to B$ is injective if $\forall x, y \in A$, if $f(x) = f(y)$, then $x = y$.
- Bijective or 1-1 correspondence: A function is bijective if it is surjective and injective.

1. $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = x^2$.
2. $f : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ such that $f(x) = x^2$.

Comparing (finite and infinite) sets



- Surjective or onto: $f : A \to B$ is surjective if $\forall y \in B$, $\exists x \in A$ such that $f(x) = y$. – If A, B finite, $|A| \geq |B|$
- Injective or 1-1: $f : A \to B$ is injective if $\forall x, y \in A$, if $f(x) = f(y)$, then $x = y$. – If A, B finite, $|A| \leq |B|$
- Bijective or 1-1 correspondence: A function is bijective if it is surjective and injective. – If A, B finite, $|A| = |B|$

1. $f : \mathbb{Z} \to \mathbb{Z}$ such that $f(x) = x^2$.
2. $f : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ such that $f(x) = x^2$.

Properties of finite and infinite sets

Relative notion of "size"

Thus, two finite/infinite sets have the same "size" iff there is a bijection between them.

Properties of finite and infinite sets

Similarities between finite and infinite sets

- $\exists$ **bij** from A to B and B to C, implies $\exists$ **bij** from A to C.
- $\exists$ **bij** from A to B, then $\exists$ **bij** from B to A.
- $\exists$ **surj** from A to B and $\exists$ **surj** B to A, implies $\exists$ **bij** from A to B.

Properties of finite and infinite sets

Similarities between finite and infinite sets

- $\exists$ **bij** from A to B and B to C, implies $\exists$ **bij** from A to C.
- $\exists$ **bij** from A to B, then $\exists$ **bij** from B to A.
- (Schröder-Bernstein Theorem:) $\exists$ **surj** from A to B and $\exists$ **surj** B to A, implies $\exists$ **bij** from A to B. (H.W: Read this!)