CS 207 Discrete Mathematics – 2013-2014

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 1: What is a proof?

July 18, 2013

Credit Structure

Course credit structure

quizzes	25%
mid-sem	35%
end-sem	40%

Office hours:	11:00am to 1:00pm (Wednesday)
Problem solving session:	1 hour per week (To be announced)

Important Announcements

Quiz 1: August 28, 2013 , Wednesday, 8:30am to 9:30am

Quiz 2: September 4, 2013 , Wednesday, 8:30am to 9:30am

Important Announcements

Quiz 1:	August 28, 2013 , Wednesday, 8:30am to 9:30am
Quiz 2:	September 4, 2013 , Wednesday, 8:30am to 9:30am
No classes on:	July 22, 2013, July 23, 2013 and July 25, 2013

Important Announcements

Quiz 1:	August 28, 2013 , Wednesday, 8:30am to 9:30am
Quiz 2:	September 4, 2013 , Wednesday, 8:30am to 9:30am
No classes on:	July 22, 2013, July 23, 2013 and July 25, 2013
Next class:	July 29, 2013

Course Outline

- Mathematical reasoning and mathematical objects
- Combinatorics
- Elements of graph theory
- Elements of abstract algebra

Course Outline

- Mathematical reasoning and mathematical objects
  - What is a proof? Types of proof methods
  - Induction
  - Sets, relations, functions, partial orders, graphs
- Combinatorics
- Elements of graph theory
- Elements of abstract algebra

Course Outline

- Mathematical reasoning and mathematical objects
  - What is a proof? Types of proof methods
  - Induction
  - Sets, relations, functions, partial orders, graphs

Text: *Discrete Mathematics and its applictions, by Kenneth Rosen*
Chapter 2 : 2.1, 2.2, 2.3, Chapter 8 : 8.1, 8.5, 8.6
Class notes: will be uploaded on Moodle

- Combinatorics
- Elements of graph theory
- Elements of abstract algebra

What is a proposition?

A statement that is either true or false.

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
  $\forall$: for all,
  $\exists$: there exists,
  $\in, \notin$: contained in, and not contained in

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
  $\forall$: for all,
  $\exists$: there exists,
  $\in, \notin$: contained in, and not contained in
  $\mathbb{N}$: the set of natural numbers,
  $\mathbb{Z}$: the set of integers,
  $\mathbb{Q}$: the set of rationals,
  $\mathbb{Z}^+$: the set of positive integers,
  $\mathbb{R}$: the set of reals

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 - b^2 = c$;

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 - b^2 = c$;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{Z} : a^2 - b^2 = c$;

It is not always easy to tell whether a proposition is true or false.

Theorems and proofs

Theorem

If $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$

Theorems and proofs

Theorem

If $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$

(scratchpad)

Theorems and proofs

Theorem

If $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$

(scratchpad)

Proof.

As $-x^3 + 4x = x(4 - x^2)$, which is in fact $x(2 - x)(2 + x)$, the quantity is ~~positive~~ non-negative for $0 \leq x \leq 2$. Adding 1 to a non-negative quantity makes it positive. Therefore, the above theorem. □

Theorems and Proofs

Given: a number $n \in \mathbb{N}$

Check: Is n prime?

Theorems and Proofs

Given: a number $n \in \mathbb{N}$
Check: Is n prime?

for $i = 2$ to $\sqrt{n}$ **do**
  if $i \mid n$ **then**
    output "no"
  end if
end for

Theorems and Proofs

Given: a number $n \in \mathbb{N}$
Check: Is n prime?

for $i = 2$ to $\sqrt{n}$ **do**
  if $i|n$ **then**
    output "no"
  end if
end for

Why is this algorithm correct?
Is there a number $n \in \mathbb{N}$ s.t
$\forall i : i \in \{2, 3, \ldots, \sqrt{n}\}\ i \nmid n$,
but $\exists j > \sqrt{n}$ s.t. $j|n$?

Is there a composite $n \in \mathbb{N}$ s.t. all its prime factors are greater than $\sqrt{n}$?

Theorems and Proofs

Is there a number $n \in \mathbb{N}$ s.t
$\forall i : i \in \{2, 3, \ldots, \sqrt{n}\}\ i \nmid n$,
but $\exists j > \sqrt{n}$ s.t. $j|n$?

Is there a composite $n \in \mathbb{N}$ s.t. all its prime factors are greater than $\sqrt{n}$?

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Proof.

As n is a composite, $\exists x, y \in \mathbb{N}, x, y < n : n = xy$. If $x > \sqrt{n}$ and $y > \sqrt{n}$ then $xy > n$. Therefore, one of x or y is less than or equal to $\sqrt{n}$. Say x is smaller than $\sqrt{n}$. It is either a composite or a prime. If it is a prime, then we are done. Else, it has prime factorization (axiom: unique factorization in $\mathbb{N}$) and again, we are done. □

Theorems and Proofs

Is there a number $n \in \mathbb{N}$ s.t
$\forall i : i \in \{2, 3, \ldots, \sqrt{n}\}\ i \nmid n$,
but $\exists j > \sqrt{n}$ s.t. $j|n$?

Is there a composite $n \in \mathbb{N}$ s.t. all its prime factors are greater than $\sqrt{n}$?

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Proof.

As n is a composite, $\exists x, y \in \mathbb{N}, x, y < n : n = xy$. If $x > \sqrt{n}$ and $y > \sqrt{n}$ then $xy > n$. Therefore, one of x or y is less than or equal to $\sqrt{n}$. Say x is smaller than $\sqrt{n}$. It is either a composite or a prime. If it is a prime, then we are done. Else, it has prime factorization (axiom: unique factorization in $\mathbb{N}$) and again, we are done. □

Axioms

Euclid in 300BC invented the method of axioms-and-proofs.

Using only a handful of axioms called Zermelo-Fraenkel and Choice (ZFC) and a few rules of deductions the entire mathematics can be deduced!

Proving theorems starting from ZFC alone is tedious. 20,000+ lines proof for $2 + 2 = 4$

We will assume a whole lot of axioms to prove theorems: all familiar facts from high school math.

Class problems

- (CW1.1) Prove that for any $n \in \mathbb{N}$, $n(n^2 - 1)(n + 2)$ is divisible by 4. (what about divisible by 8?)
- (CW1.2) Prove that for any $n \in \mathbb{N}$, $2^n < (n + 2)!$

Bogus proofs

Theorem (Bogus)

$1/8 > 1/4$

Proof.

$$3 > 2$$
$$3 \log_{10}(1/2) > 2 \log_{10}(1/2)$$
$$\log_{10}(1/2)^3 > \log_{10}(1/2)^2$$
$$(1/2)^3 > (1/2)^2$$

Another bogus proof

Theorem

For all non-negative numbers a, b $\frac{a+b}{2} \geq \sqrt{ab}$

Proof.

$$\frac{a+b}{2} \geq^{?} \sqrt{ab}$$

$$a+b \geq^{?} 2\sqrt{ab}$$

$$a^2+2ab+b^2 \geq^{?} 4ab$$

$$a^2-2ab+b^2 \geq^{?} 0$$

$$(a-b)^2 \geq 0$$

□

Proof Methods

Proof by contrapositive

Theorem

If r is irrational then $\sqrt{r}$ is also irrational.

Proof by contrapositive

Theorem

If r is irrational then $\sqrt{r}$ is also irrational.

Definition (Contrapozitive)

The contrapositive of "if P then Q" is "if $\neg Q$ then $\neg P$"

Proof by contrapositive

Theorem

If r is irrational then $\sqrt{r}$ is also irrational.
If $\sqrt{r}$ is rational then r is rational.

Proof.

Suppose $\sqrt{r}$ is rational. Then $\sqrt{r} = p/q$ for $p, q \in \mathbb{Z}$. Therefore, $r = p^2/q^2$. □

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof by contradiction

Theorem

$\sqrt{2}$ is irrational.

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even.

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. (CW2.1) If p^2 is even, then p is even.

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even.
If p^2 is even, then p is even. (why?)
Suppose not, i..e p^2 is even but p is not. Then $p = 2k + 1$ for some integer k. $p^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. As $4(k^2 + k)$ is even, $4k^2 + 4k + 1$ is odd, which is a contradiction.

Proof by contradiction

Theorem

$\sqrt{2}$ is irrational.

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. If p^2 is even, then p is even.

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. If p^2 is even, then p is even. Therefore, $p = 2k$ for some $k \in \mathbb{Z} \Rightarrow$ $2q^2 = 4k^2 \Rightarrow q^2 = 2k^2 \Rightarrow q^2$ is even. Therefore, q is even. That is, p, q have a common factor. This leads to a contradiction. □

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. If p^2 is even, then p is even. Therefore, $p = 2k$ for some $k \in \mathbb{Z} \Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2k^2 \Rightarrow q^2$ is even. Therefore, q is even. That is, p, q have a common factor. This leads to a contradiction. □

(CW2.2) Prove that there are infinitely many primes.

Well-ordering principle and Induction

Axiom (WOP)

Every nonempty set of non-negative integers has a smallest element.

Well-ordering principle and Induction

Axiom (WOP)

Every nonempty set of non-negative integers has a smallest element.

Axiom (Induction)

Let $P(n)$ be a property of non-negative integers. If

1. *$P(0)$ is true (Base case)*
2. *for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$ (Induction step)*

then $P(n)$ is true for for all $n \in \mathbb{N}$.

Well-ordering principle and Induction

Axiom (WOP)

Every nonempty set of non-negative integers has a smallest element.

Axiom (Induction)

Let $P(n)$ be a property of non-negative integers. If

1. *$P(0)$ is true (Base case)*
2. *for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$ (Induction step)*

then $P(n)$ is true for for all $n \in \mathbb{N}$.

Axiom (Strong Induction)

Let $P(n)$ be a property of non-negative integers. If

1. *$P(0)$ is true (Base case)*
2. *$[\forall k \in \{0, 1, \ldots, n\} : P(k)] \Rightarrow P(n+1)$ (Induction step)*

then $P(n)$ is true for for all $n \in \mathbb{N}$.

WOP $\Rightarrow$ Induction

Theorem

Well-ordering principle implies Induction

Proof.

Let $P(0)$ be true and for each $n \geq 0$, let $P(n) \Rightarrow P(n+1)$.
Let us assume for the sake of contradiction that $P(n)$ is not true for all positive integers.
Let $C = \{i \mid P(i) \text{ is false}\}$. As C is non-empty and non-negative integers C has a smallest element (due to WOP), say i_0.
Now, $i_0 \neq 0$. Also $P(i_0 - 1)$ is true, as $i_0 - 1$ is not in C. But $P(i_0 - 1) \Rightarrow P(i_0)$, which is a contradiction. $\square$

WOP $\Rightarrow$ Induction

Theorem

Well-ordering principle implies Induction

Proof.

Let $P(0)$ be true and for each $n \geq 0$, let $P(n) \Rightarrow P(n+1)$.
Let us assume for the sake of contradiction that $P(n)$ is not true for all positive integers.
Let $C = \{i \mid P(i) \text{ is false}\}$. As C is non-empty and non-negative integers C has a smallest element (due to WOP), say i_0.
Now, $i_0 \neq 0$. Also $P(i_0 - 1)$ is true, as $i_0 - 1$ is not in C. But $P(i_0 - 1) \Rightarrow P(i_0)$, which is a contradiction. $\square$

Theorem

WOP $\Leftrightarrow$ Induction $\Leftrightarrow$ Strong Induction [HW]

Using Induction to prove theorems

Theorem

$2^n \leq (n+1)!$

Proof.

Base case ($n = 0$): $2^0 = 1 = 1!$

Using Induction to prove theorems

Theorem

$2^n \leq (n+1)!$

Proof.

Base case ($n = 0$): $2^0 = 1 = 1!$
Induction hypothesis: $2^n \leq (n+1)!$.

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &\leq 2 \cdot (n+1)! \text{ (by indiction hypothesis)} \\ &\leq (n+2) \cdot (n+1)! \\ &\leq (n+2)! \end{aligned}$$

□

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
(Such an s exists due to WOP.)

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.
And, now we can repeat the argument with respect to A.
Therefore, if (A, B, C) is a solution then so is (α, β, γ).

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.
And, now we can repeat the argument with respect to A.
Therefore, if (A, B, C) is a solution then so is (α, β, γ).
But $\beta < B$, which is a contradiction.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

It is not always as easy to prove such theorems.

Conjecture (Euler, 1769)

There are no positive integer solutions over $\mathbb{Z}$ *to the equation:*

$$a^4 + b^4 + c^4 = d^4$$

Integer values for a, b, c, d that do satisfy this equation were first discovered in 1986.
It took more two hundred years to prove it.

CS 207 Discrete Mathematics – 2012-2013

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 2: Well-ordering principle and Induction

July 29, 2013

CS 207 Discrete Mathematics – 2012-2013

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 2: Well-ordering principle and Induction

July 29, 2013

Last time

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
  - If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
  - If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
  - If r is irrational then $\sqrt{r}$ is irrational.

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
  - If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
  - If r is irrational then $\sqrt{r}$ is irrational.
  - $\sqrt{2}$ is irrational.

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
  - If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
  - If r is irrational then $\sqrt{r}$ is irrational.
  - $\sqrt{2}$ is irrational.
  - Well-ordering principle implies induction.

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
  - If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
  - If r is irrational then $\sqrt{r}$ is irrational.
  - $\sqrt{2}$ is irrational.
  - Well-ordering principle implies induction.
  - $2^n < n!$

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
  - If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.
  - If r is irrational then $\sqrt{r}$ is irrational.
  - $\sqrt{2}$ is irrational.
  - Well-ordering principle implies induction.
  - $2^n < n!$
- The well ordering principle, induction, and strong induction.

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
- The well ordering principle, induction, and strong induction.

You were asked to think about the following problem:

- Is $2^n < \frac{n}{2}!$?

Recap

- What are axioms, propositions, theorems, claims and proofs?
- Various theorems we proved in class:
- The well ordering principle, induction, and strong induction.

You were asked to think about the following problem:

- Is $2^n < \frac{n}{2}!$?
- Try to also think about the following: (CW2.1)
  For every positive integer n there exists another positive integer k such that n is of the form $9k, 9k+1$, or $9k-1$.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let $s = (A, B, C)$ be the solution with the smallest value of b in S.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let $s = (A, B, C)$ be the solution with the smallest value of b in S.
(Such an s exists due to WOP.)

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let $s = (A, B, C)$ be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let $s = (A, B, C)$ be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let $s = (A, B, C)$ be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.
And, now we can repeat the argument with respect to A.
Therefore, if (A, B, C) is a solution then so is (α, β, γ).

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let $s = (A, B, C)$ be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.
And, now we can repeat the argument with respect to A.
Therefore, if (A, B, C) is a solution then so is (α, β, γ).
But $\beta < B$, which is a contradiction.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

It is not always as easy to prove such theorems.

Conjecture (Euler, 1769)

There are no positive integer solutions over $\mathbb{Z}$ *to the equation:*

$$a^4 + b^4 + c^4 = d^4$$

Integer values for a, b, c, d that do satisfy this equation were first discovered in 1986.
It took more two hundred years to prove it.

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ *prove that*

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3$$

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ *prove that*

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3$$

scratch pad

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ *prove that*

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3$$

scratch pad

a slightly stronger induction hypothesis is required

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ prove that

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3$$

Proof.

For all $2 \leq i \leq j, i, j \in \mathbb{N}$ let $f(i,j) = \sqrt{i\sqrt{i+1\ldots\sqrt{j}}}$.
We will prove a slightly more general statement:
For all $2 \leq i \leq j, i, j \in \mathbb{N}, f(i,j) < i+1$
This is more general than the theorem statement we wanted to prove.

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ *prove that*

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3 \Leftarrow \forall 2 \leq i < j, i, j \in \mathbb{N}, f(i,j) < i+1 \quad (*)$$

Proof.

For all $2 \leq i \leq j, i, j \in \mathbb{N}$ let $f(i,j) = \sqrt{i\sqrt{i+1\ldots\sqrt{j}}}$.

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ *prove that*

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3 \Leftarrow \forall 2 \leq i < j, i, j \in \mathbb{N}, f(i,j) < i+1 \quad (*)$$

Proof.

For all $2 \leq i \leq j, i, j \in \mathbb{N}$ let $f(i,j) = \sqrt{i\sqrt{i+1\ldots\sqrt{j}}}$.
We prove $(*)$ by induction on $j - i$.

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ prove that

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3 \Leftarrow \forall 2 \leq i < j, i, j \in \mathbb{N}, f(i,j) < i+1 \quad (*)$$

Proof.

For all $2 \leq i \leq j, i, j \in \mathbb{N}$ let $f(i,j) = \sqrt{i\sqrt{i+1\ldots\sqrt{j}}}$.
We prove $(*)$ by induction on $j - i$.
Base case: $j - i = 1$. $f(i, i+1) = \sqrt{i\sqrt{i+1}} < i+1$.

A proof by induction

Theorem

For any $n \in \mathbb{N}, n \geq 2$ prove that

$$\sqrt{2\sqrt{3\sqrt{4\ldots\sqrt{n-1\sqrt{n}}}}} < 3 \Leftarrow \forall 2 \leq i < j, i, j \in \mathbb{N}, f(i,j) < i+1 \quad (*)$$

Proof.

For all $2 \leq i \leq j, i, j \in \mathbb{N}$ let $f(i,j) = \sqrt{i\sqrt{i+1\ldots\sqrt{j}}}$.
We prove $(*)$ by induction on $j - i$.
Base case: $j - i = 1$. $f(i, i+1) = \sqrt{i\sqrt{i+1}} < i+1$.
Induction:

$$\begin{aligned} f(i,j+1) &= \sqrt{i \cdot f(i+1,j+1)} \\ &< \sqrt{i \cdot (i+2)} && \text{(by Induction Hypothesis)} \\ &\leq i+1 && \text{(by AM-GM inequality)} \end{aligned}$$

A Bogus Inductive proof

Theorem (Bogus, CW2.2)

$a \in \mathbb{R}$, $a > 0$. *Then*, $\forall n \in \mathbb{N}$, $a^n = 1$.

A Bogus Inductive proof

Theorem (Bogus, CW2.2)

$a \in \mathbb{R}$, $a > 0$. *Then*, $\forall n \in \mathbb{N}$, $a^n = 1$.

By Strong Induction.

Base case: $n = 0$. So $a^n = 1$.

A Bogus Inductive proof

Theorem (Bogus, CW2.2)

$a \in \mathbb{R}$, $a > 0$. *Then*, $\forall n \in \mathbb{N}$, $a^n = 1$.

By Strong Induction.

Base case: $n = 0$. So $a^n = 1$.

Induction: $n \to n + 1$.

A Bogus Inductive proof

Theorem (Bogus, CW2.2)

$a \in \mathbb{R}$, $a > 0$. *Then*, $\forall n \in \mathbb{N}$, $a^n = 1$.

By Strong Induction.

Base case: $n = 0$. So $a^n = 1$.

Induction: $n \to n + 1$.

$$a^{n+1} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1$$

A Bogus Inductive proof

Theorem (Bogus, CW2.2)

$a \in \mathbb{R}$, $a > 0$. *Then*, $\forall n \in \mathbb{N}$, $a^n = 1$.

By Strong Induction.

Base case: $n = 0$. So $a^n = 1$.

Induction: $n \to n + 1$.

$$a^{n+1} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1$$

???

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 well-ordering principle.

Recap

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

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 properties that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$ and for every $a \in A$ there a $b \in B$ such that $(a, b) \in f$.

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 properties that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$ and for every $a \in A$ there a $b \in B$ such that $(a, b) \in f$.

- 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 properties that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$ and for every $a \in A$ there a $b \in B$ such that $(a, b) \in f$.

- 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, $f : A \to B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional properties that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$ and for every $a \in A$ there a $b \in B$ such that $(a, b) \in f$.

- 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 properties that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$ and for every $a \in A$ there a $b \in B$ such that $(a, b) \in f$.

- 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, $f : A \to B$, is a set defined as follows:
$f = \{(a, b) \mid a \in A, b \in B\}$ with an additional properties that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$ and for every $a \in A$ there a $b \in B$ such that $(a, b) \in f$.

- 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 properties that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$ and for every $a \in A$ there a $b \in B$ such that $(a, b) \in f$.

- 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 $f : A \to B$ 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?
  - What about $f : \mathbb{Z} \to \mathbb{Z}$, 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 $f : A \to B$ 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 $f : A \to B$ 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 $f : \mathbb{Z} \to \mathbb{N}$

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

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 $f : \mathbb{Z} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
  $f(x, y) = \left(\sum_{i=1}^{x+y} i\right) + y + 1$

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 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

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 $f : \mathbb{Z} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
  CW

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 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- Is there a bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$?

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 $f : \mathbb{Z} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- Is there a bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$?
- Is there a bijection between $\mathbb{R}$ and $\mathbb{N}$?

CS 207 Discrete Mathematics – 2013-2014

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 4: Properties of infinite sets

Aug 1, 2013

Last time

Recap

- How to define sets?
- What are finite and infinite sets?

Recap

- How to define sets?
- What are finite and infinite sets?
- What are functions?

Recap

- How to define sets?
- What are finite and infinite sets?
- What are functions? What are injective, surjective, and bijective functions?

Recap

- How to define sets?
- What are finite and infinite sets?
- What are functions? What are injective, surjective, and bijective functions?
- Comparing sizes of infinite sets.

Size of 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

Size of 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 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Size of 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 $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- There is a bijection $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$
- Is there a bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$?
- Is there a bijection between $\mathbb{R}$ and $\mathbb{N}$?

Finite sets vs infinite sets

On the one hand

- If A is finite then there is no bijection from $A \times A$ to A. Whereas if A is countably infinite

Finite sets vs infinite sets

On the one hand

- If A is finite then there is no bijection from $A \times A$ to A. Whereas if A is countably infinite, where A is said to be countably infinite if there is a bijection from A to $\mathbb{N}$

Finite sets vs infinite sets

On the one hand

- If A is finite then there is no bijection from $A \times A$ to A. Whereas if A is countably infinite then there is a bijection from $A \times A$ to A

Finite sets vs infinite sets

On the one hand

- If A is finite then there is no bijection from $A \times A$ to A. Whereas if A is countably infinite then there is a bijection from $A \times A$ to A

On the other hand

Finite sets vs infinite sets

On the one hand

- If A is finite then there is no bijection from $A \times A$ to A. Whereas if A is countably infinite then there is a bijection from $A \times A$ to A

On the other hand

- Today we will see two theorems which prove two properties of infinite sets that they share with finite sets.

Finite sets vs infinite sets

On the one hand

- If A is finite then there is no bijection from $A \times A$ to A. Whereas if A is countably infinite then there is a bijection from $A \times A$ to A

On the other hand

- Today we will see two theorems which prove two properties of infinite sets that they share with finite sets.

Theorem (Cantor, 1891)

There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$.

Finite sets vs infinite sets

On the one hand

- If A is finite then there is no bijection from $A \times A$ to A. Whereas if A is countably infinite then there is a bijection from $A \times A$ to A

On the other hand

- Today we will see two theorems which prove two properties of infinite sets that they share with finite sets.

Theorem (Cantor, 1891)

There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$.

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

Cantor's diagonalisation

Theorem (Cantor, 1891)

There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$.

Proof.

Suppose for the sake of contradiction that there is a bijection, say f, between set of all subsets of $\mathbb{N}$.

	0	1	2	3	...
$\emptyset$					
$\{1\}$					
$\{2\}$					
$\{1,2\}$					
:					
:					

Cantor's diagonalisation

Theorem (Cantor, 1891)

There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$.

Proof.

Suppose for the sake of contradiction that there is a bijection, say f, between set of all subsets of $\mathbb{N}$.

	0	1	2	3	...
$\emptyset$	✗	✗	✗	✗	...
$\{1\}$	✗	✓	✗	✗	...
$\{2\}$	✗	✗	✓	✗	...
$\{1,2\}$	✗	✓	✓	✗	...
⋮	...	...	...	...	...
⋮	...	...	...	...	...

Cantor's diagonalisation

Theorem (Cantor, 1891)

There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$.

Proof.

Suppose for the sake of contradiction that there is a bijection, say f, between set of all subsets of $\mathbb{N}$.

	0	1	2	3	...
$\emptyset$	✓	✗	✗	✗	...
$\{1\}$	✗	✗	✗	✗	...
$\{2\}$	✗	✗	✗	✗	...
$\{1,2\}$	✗	✓	✓	✓	...
:	...	...	...	...	...
:	...	...	...	...	...

Cantor's diagonalisation

Theorem (Cantor, 1891)

There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$.

Proof.

Suppose for the sake of contradiction that there is a bijection, say f, between set of all subsets of $\mathbb{N}$.

	0	1	2	3	...
$\emptyset$	✓	✗	✗	✗	...
$\{1\}$	✗	✗	✗	✗	...
$\{2\}$	✗	✗	✗	✗	...
$\{1,2\}$	✗	✓	✓	✓	...
:	...	...	...	...	...
:	...	...	...	...	...

The inverted diagonal set does not belong to any of the existing sets! □

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:
Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}, h(x) = x + 1$.

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:
Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}, h(x) = x + 1$.
Why are g, h injective? Are they bijective?

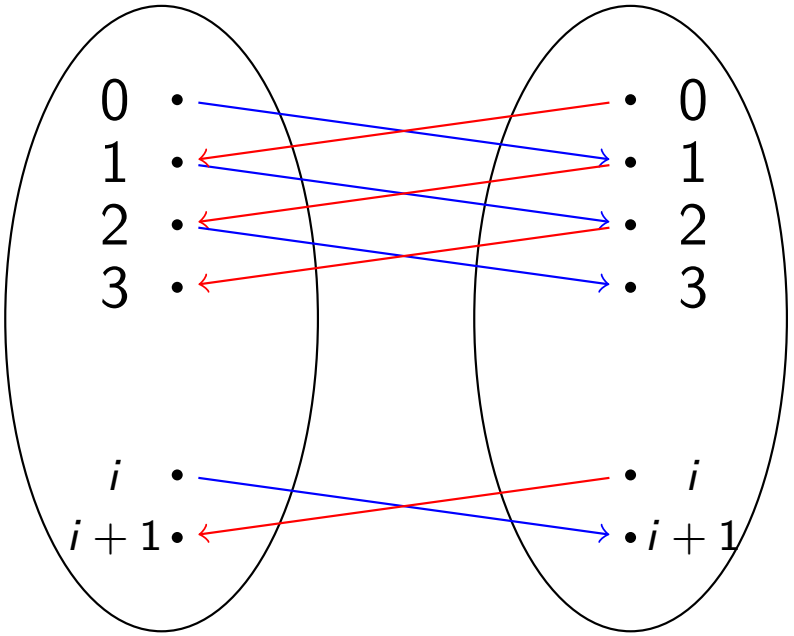
Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:

Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}$, $h(x) = x + 1$.



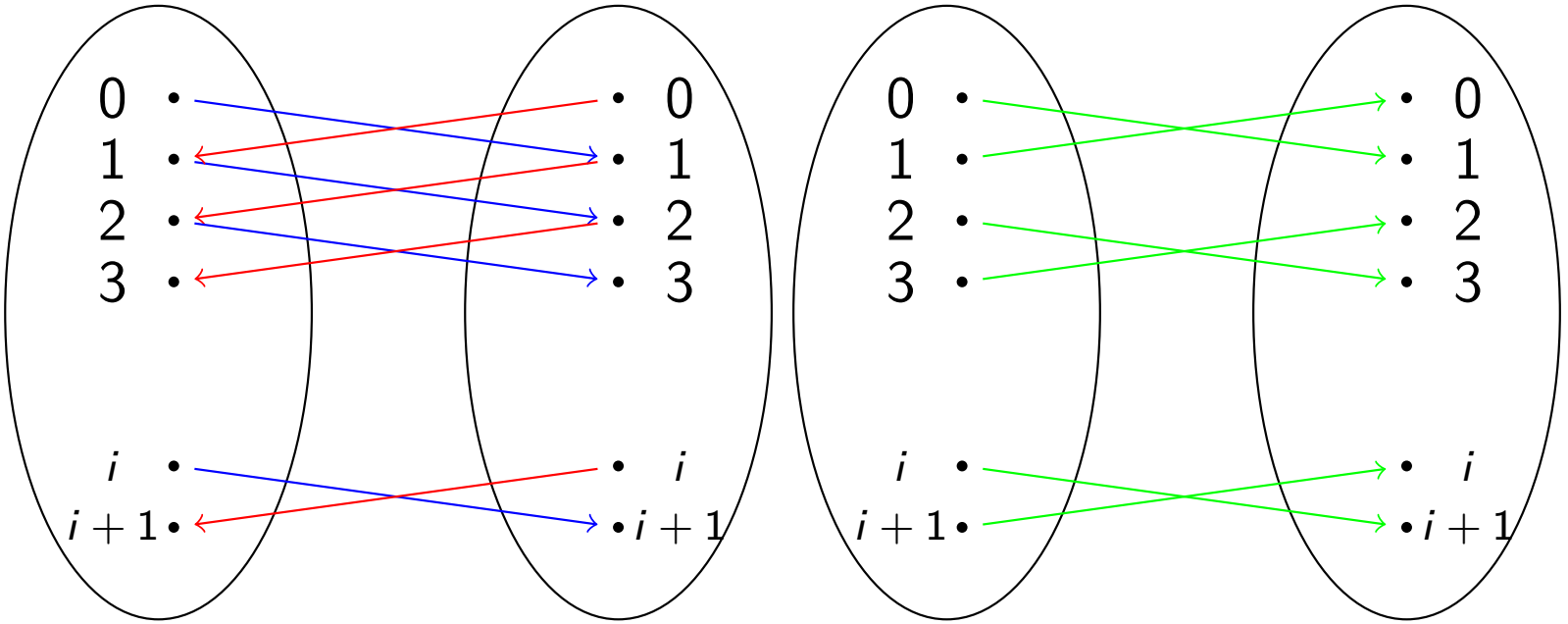
Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:

Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}$, $h(x) = x + 1$.



CS 207 Discrete Mathematics – 2013-2014

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 5: Schroder-Bernstein

Aug 5, 2013

Recap

- There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$.

Recap

- There is no bijection between $\mathbb{N}$ and set of all subsets of $\mathbb{N}$. Proof by Cantor's diagonalization. [Cantor, 1891]

Today

- Another property of sets which holds for both finite and infinite sets. [Schröder-Bernstein Theorem]

Today

- Another property of sets which holds for both finite and infinite sets. [Schröder-Bernstein Theorem]
- An interesting game and an open problem (If time permits).

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:
Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}, h(x) = x + 1$.

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:
Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}, h(x) = x + 1$.
Why are g, h injective? Are they bijective?

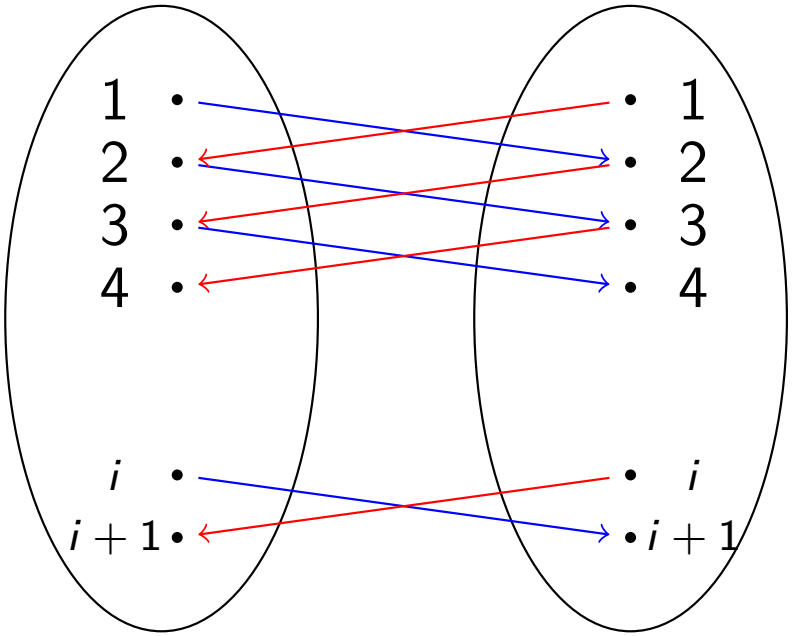
Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:

Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}$, $h(x) = x + 1$.



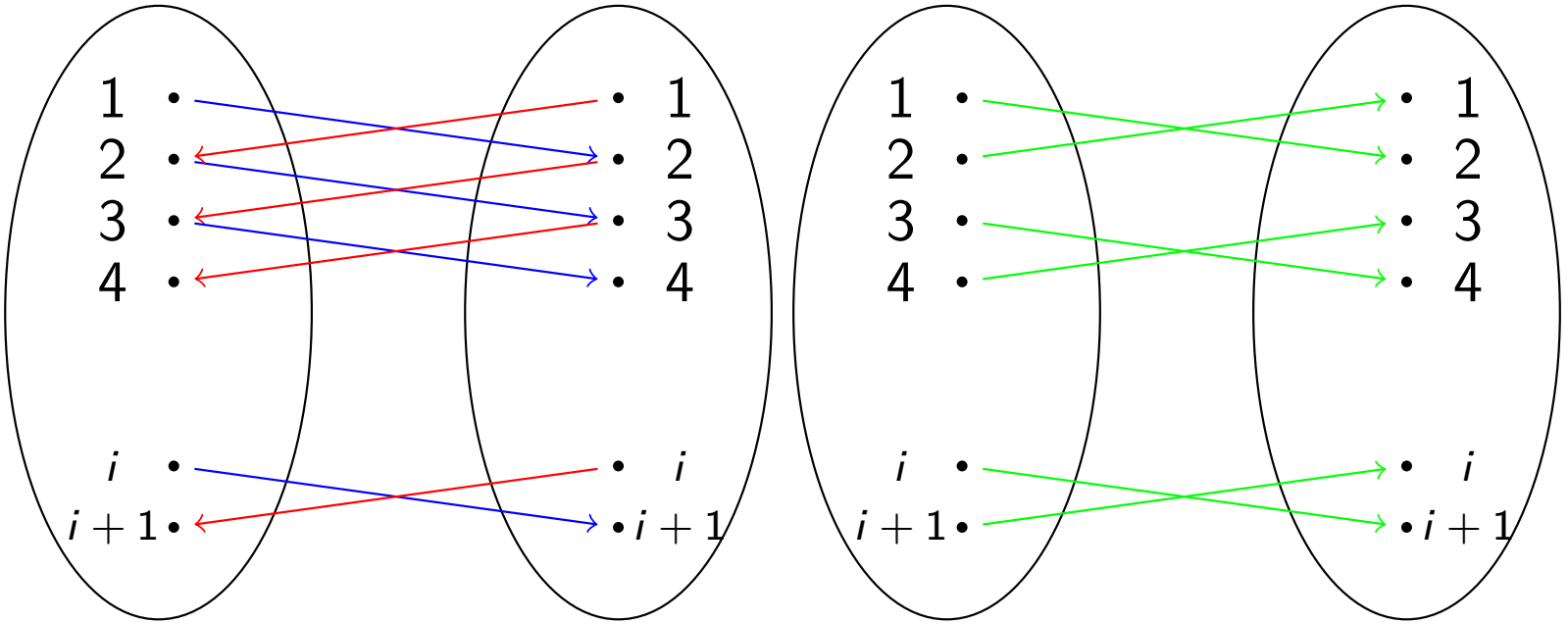
Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

A toy example:

Say $g : \mathbb{N} \to \mathbb{N}$, $g(x) = x+1$ and $h : \mathbb{N} \to \mathbb{N}$, $h(x) = x + 1$.



Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

There are two types of elements in B.

- $B_0 = \{b \in B \mid \exists a \in A \text{ s.t. } g(a) = b\}$
- $B_1 = \{b \in B \mid \nexists a \in A \text{ s.t. } g(a) = b\}$

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

There are two types of elements in B.

- $B_0 = \{b \in B \mid \exists a \in A \text{ s.t. } g(a) = b\}$
- $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

There are two types of elements in B.

- $B_0 = \{b \in B \mid \exists a \in A \text{ s.t. } g(a) = b\}$
- $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$

An element $b \in B$ be called h-good if $\exists \beta \in B_1, \exists n \in \mathbb{N}$ s.t. $b = (g \odot h)^n \beta$

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

There are two types of elements in B.

- $B_0 = \{b \in B \mid \exists a \in A \text{ s.t. } g(a) = b\}$
- $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$

An element $b \in B$ be called h-good if $\exists \beta \in B_1, \exists n \in \mathbb{N}$ s.t. $b = (g \odot h)^n \beta$
What is $(f \odot g)^n$? What does it mean to be h-good?

Schröder-Bernstein

Theorem

Let A, B be two sets. If there is a injective map g from A to B and another injective map h from B to A then there is a bijection between A, B.

There are two types of elements in B.

- $B_0 = \{b \in B \mid \exists a \in A \text{ s.t. } g(a) = b\}$
- $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$

An element $b \in B$ be called h-good if $\exists \beta \in B_1, \exists n \in \mathbb{N}$ s.t. $b = (g \odot h)^n \beta$

We now define another map from A to B as follows:

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

To finish the proof, we will prove the following lemma about f.

Lemma

The map f defined above is a bijection.

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is h-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.
Case 1 [$g(a), g(a')$ are h-good:] then $f(a) = h^{-1}(a) = f(a') = h^{-1}(a')$.
Say $h^{-1}(a) = b_0$. Then we have, $h(b_0) = a$ and $h(b_0) = a'$, i.e. h is not a well-defined functions. This is a contradiction.

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.
Case 2 [$g(a), g(a')$ are not h-good:] then $f(a) = g(a) = f(a') = g(a')$.
Then we have, $g(a) = g(a')$, i.e. g is not injective. This is a contradiction.

□

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.

Case 3[only $g(a)$ is h-good:] We have that $f(a) = f(a')$.

As $g(a)$ is h-good, $f(a) = h^{-1}(a)$. As $g(a')$ is not h-good, $f(a') = g(a')$.

□

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.
Case 3[only $g(a)$ is h-good:] We have that $f(a) = f(a')$.
As $g(a)$ is h-good, $f(a) = h^{-1}(a)$. As $g(a')$ is not h-good, $f(a') = g(a')$.
Therefore, $h^{-1}(a) = g(a')$. Call this element b^*.

□

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.

Case 3[only $g(a)$ is h-good:] We have that $f(a) = f(a')$.

As $g(a)$ is h-good, $f(a) = h^{-1}(a)$. As $g(a')$ is not h-good, $f(a') = g(a')$.

Therefore, $h^{-1}(a) = g(a')$. Call this element b^*.

As $g(a') = b^*$, $b^* \notin B_1$. But as $g(a)$ is h-good. Therefore,

$(h \odot g)^{-i}(b^*) \in B_1$ for some $i \in \mathbb{N}$.

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.

Case 3[only $g(a)$ is h-good:] We have that $f(a) = f(a')$.

As $g(a)$ is h-good, $f(a) = h^{-1}(a)$. As $g(a')$ is not h-good, $f(a') = g(a')$.

Therefore, $h^{-1}(a) = g(a')$. Call this element b^*.

As $g(a') = b^*$, $b^* \notin B_1$. But as $g(a)$ is h-good. Therefore,

$(h \odot g)^{-i}(b^*) \in B_1$ for some $i \in \mathbb{N}$.

Assuming $g(a')$ is not h-good, paths walked backwards from b^* lead to B_0.

But Assuming $g(a)$ is h-good, paths walked backwards from b^* lead to B_1.

□

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is } h\text{-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is injective from* A *to* B

Proof.

Suppose (for the sake of contradiction) $a \neq a'$ and $f(a) = f(a')$.

Case 3[only $g(a)$ is h-good:] We have that $f(a) = f(a')$.

As $g(a)$ is h-good, $f(a) = h^{-1}(a)$. As $g(a')$ is not h-good, $f(a') = g(a')$.

Therefore, $h^{-1}(a) = g(a')$. Call this element b^*.

As $g(a') = b^*$, $b^* \notin B_1$. But as $g(a)$ is h-good. Therefore,

$(h \odot g)^{-i}(b^*) \in B_1$ for some $i \in \mathbb{N}$.

Assuming $g(a')$ is not h-good, paths walked backwards from b^* lead to B_0.

But Assuming $g(a)$ is h-good, paths walked backwards from b^* lead to B_1.

Contradiction! □

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is h-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is surjective from* A *to* B

Schröder-Bernstein

Lemma

Let $B_1 = \{b \in B \mid \forall a \in A \text{ s.t. } g(a) \neq b\}$, *and*

$$f(a) = \begin{cases} h^{-1}(a) & \text{if } g(a) \text{ is h-good} \\ g(a) & \text{otherwise} \end{cases}$$

Then f *is surjective from* A *to* B

Proof.

HW □

Subset Take-away Game – David Gale

I am player 1 and you are player 2. We both have been given a set A. In each round, first I choose one subset of A and then you choose another subset of A. We stick to the following rules:

1. We do not choose the empty set
2. We do not choose the entire set A
3. We do not choose any superset of a set chosen in any earlier round.

First player unable to pick loses the game.

Subset Take-away Game – David Gale

I am player 1 and you are player 2. We both have been given a set A. In each round, first I choose one subset of A and then you choose another subset of A. We stick to the following rules:

1. We do not choose the empty set
2. We do not choose the entire set A
3. We do not choose any superset of a set chosen in any earlier round.

First player unable to pick loses the game.
If $|A| = 1$ then I lose.

Subset Take-away Game – David Gale

I am player 1 and you are player 2. We both have been given a set A. In each round, first I choose one subset of A and then you choose another subset of A. We stick to the following rules:

1. We do not choose the empty set
2. We do not choose the entire set A
3. We do not choose any superset of a set chosen in any earlier round.

First player unable to pick loses the game.
If $|A| = 1$ then I lose. If $|A| = 2$ then you will always win.

Subset Take-away Game – David Gale

I am player 1 and you are player 2. We both have been given a set A. In each round, first I choose one subset of A and then you choose another subset of A. We stick to the following rules:

1. We do not choose the empty set
2. We do not choose the entire set A
3. We do not choose any superset of a set chosen in any earlier round.

First player unable to pick loses the game.
If $|A| = 1$ then I lose. If $|A| = 2$ then you will always win. If $|A| = 3$ then again you can win. What happens when $|A| = 4$?

Subset Take-away Game – David Gale

I am player 1 and you are player 2. We both have been given a set A. In each round, first I choose one subset of A and then you choose another subset of A. We stick to the following rules:

1. We do not choose the empty set
2. We do not choose the entire set A
3. We do not choose any superset of a set chosen in any earlier round.

First player unable to pick loses the game.
If $|A| = 1$ then I lose. If $|A| = 2$ then you will always win. If $|A| = 3$ then again you can win. What happens when $|A| = 4$?

(Source – Mathematics for Computer Science, 2012, by Eric Lehman and F Thomson Leighton)

CS 207 Discrete Mathematics – 2013-2014

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 6: Relations

Aug 06, 2013

Last few classes

Recap

- Proofs, proof methods.

Recap

- Proofs, proof methods.
- Sets and properties of sets

Recap

- Proofs, proof methods.
- Sets and properties of sets
- Functions, properties of functions

Recap

- Proofs, proof methods.
- Sets and properties of sets
- Functions, properties of functions
- Infinite sets and properties of infinite sets.

Today

- Relations: generalisations of functions

Today

- Relations: generalisations of functions
- Types and properties of relations

Today

- Relations: generalisations of functions
- Types and properties of relations
- Representation of functions - directed graphs

What are relations?

Relation are used to talk about elements of a set.
A relation R from set A to set B, $R(A, B)$ is a subset of $A \times B$.

What are relations?

Relation are used to talk about elements of a set.
A relation R from set A to set B, $R(A, B)$ is a subset of $A \times B$.
If $A = B$ for some relation, we denote the relation as $R(A)$.

What are relations?

Relation are used to talk about elements of a set.
A relation R from set A to set B, $R(A, B)$ is a subset of $A \times B$.
If $A = B$ for some relation, we denote the relation as $R(A)$.

Examples:

- A function is a special case of a relation.

What are relations?

Relation are used to talk about elements of a set.
A relation R from set A to set B, $R(A, B)$ is a subset of $A \times B$.
If $A = B$ for some relation, we denote the relation as $R(A)$.

Examples:

- A function is a special case of a relation.
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$. R is a relation on the set of integers under which aRb holds for two numbers $a, b \in \mathbb{Z}$ if and only if $a \leq b$.

What are relations?

Relation are used to talk about elements of a set.
A relation R from set A to set B, $R(A, B)$ is a subset of $A \times B$.
If $A = B$ for some relation, we denote the relation as $R(A)$.

Examples:

- A function is a special case of a relation.
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$. R is a relation on the set of integers under which aRb holds for two numbers $a, b \in \mathbb{Z}$ if and only if $a \leq b$.
  We use aRb to denote a is related to b.

What are relations?

Relation are used to talk about elements of a set.
A relation R from set A to set B, $R(A, B)$ is a subset of $A \times B$.
If $A = B$ for some relation, we denote the relation as $R(A)$.

Examples:

- A function is a special case of a relation.
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$. R is a relation on the set of integers under which aRb holds for two numbers $a, b \in \mathbb{Z}$ if and only if $a \leq b$.
- Let S be a set $R(\mathcal{P}(S)) = \{(A, B) \mid A, B \in \mathcal{P}(S) \text{ and } A \subseteq B\}$.

What are relations?

Relation are used to talk about elements of a set.
A relation R from set A to set B, $R(A, B)$ is a subset of $A \times B$.
If $A = B$ for some relation, we denote the relation as $R(A)$.

Examples:

- A function is a special case of a relation.
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$. R is a relation on the set of integers under which aRb holds for two numbers $a, b \in \mathbb{Z}$ if and only if $a \leq b$.
- Let S be a set $R(\mathcal{P}(S)) = \{(A, B) \mid A, B \in \mathcal{P}(S) \text{ and } A \subseteq B\}$.
- Relational databases: practical examples of relations.

Properties of relations

Here we list a few definitions which define different types of relations. Let A be a set and let $R(A)$ be a relation on A.

- Reflexive:

Properties of relations

Here we list a few definitions which define different types of relations. Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if $aRa \; \forall a \in A$.

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if $aRa\ \forall a \in A$.
  - Is $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$ reflexive?
  - Is $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a < b\}$ reflexive?
  - Is $R(\mathcal{P}(S)) = \{(A, B) \mid A, B \in \mathcal{P}(S), A \subseteq B\}$?

Properties of relations

Here we list a few definitions which define different types of relations. Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if $aRa \; \forall a \in A$.
- Symmetric:

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
  - Is $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$ symmetric?
  - Is $R(\text{YourClass}) = \{(a, b) \mid a, b \in \text{YourClass and } a \text{ friend of } b\}$ symmetric?
  - Is $R(\mathcal{P}(S)) = \{(A, B) \mid A \cap B = \emptyset\}$ symmetric?

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
- Transitive:

Properties of relations

Here we list a few definitions which define different types of relations. Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
- Transitive: $R(A)$ is called transitive if $\forall a, b, c \in A$ aRb and bRc implies aRc.

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
- Transitive: $R(A)$ is called transitive if $\forall a, b, c \in A$ aRb and bRc implies aRc.
  - Is $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$ transitive?
  - Is $R(\mathbb{N}) = \{(a, b) \mid a \ (mod \ b) \neq 0\}$ transitive?
  - Is $R(\mathcal{P}(S)) = \{(A, B) \mid A \subseteq B\}$ transitive?

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
- Transitive: $R(A)$ is called transitive if $\forall a, b, c \in A$ aRb and bRc implies aRc.
- Anti-symmetric:

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
- Transitive: $R(A)$ is called transitive if $\forall a, b, c \in A$ aRb and bRc implies aRc.
- Anti-symmetric: $R(A)$ is called anti-symmetric if $\forall a, b \in A$ aRb and bRa implies $a = b$.

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
- Transitive: $R(A)$ is called transitive if $\forall a, b, c \in A$ aRb and bRc implies aRc.
- Anti-symmetric: $R(A)$ is called anti-symmetric if $\forall a, b \in A$ aRb and bRa implies $a = b$.
  - Is $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$ anti-symmetric?
  - Is $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a|b\}$ anti-symmetric?
  - Is $R(\mathcal{P}(S)) = \{(A, B) \mid A \subseteq B\}$ anti-symmetric?

Properties of relations

Here we list a few definitions which define different types of relations.
Let A be a set and let $R(A)$ be a relation on A.

- Reflexive: $R(A)$ is called reflexive if aRa $\forall a \in A$.
- Symmetric: $R(A)$ is called symmetric if $\forall a, b \in A$ aRb implies bRa.
- Transitive: $R(A)$ is called transitive if $\forall a, b, c \in A$ aRb and bRc implies aRc.
- Anti-symmetric: $R(A)$ is called anti-symmetric if $\forall a, b \in A$ aRb and bRa implies $a = b$.

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \ (mod \ n)\}$

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \ (mod \ n)\}$
- $R(\Sigma^*) = \{(x, y) \mid x, y \in \Sigma^* \text{ and } x = \text{suff}(y)\}$

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \ (mod \ n)\}$
- $R(\Sigma^*) = \{(x, y) \mid x, y \in \Sigma^* \text{ and } x = \text{suff}(y)\}$
  Σ is a finite alphabet. Σ^* are strings of arbitrary length over Σ

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \ (mod \ n)\}$
- $R(\Sigma^*) = \{(x, y) \mid x, y \in \Sigma^* \text{ and } x = \text{suff}(y)\}$
- $R(\mathbb{N}) = \{(a, b) \mid a \ (mod \ b) \neq 0\}$

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \ (mod \ n)\}$
- $R(\Sigma^*) = \{(x, y) \mid x, y \in \Sigma^* \text{ and } x = \text{suff}(y)\}$
- $R(\mathbb{N}) = \{(a, b) \mid a \ (mod \ b) \neq 0\}$
- $R(\mathbb{R}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a^2 \leq b^2\}$

Types of relations

We will study the following two types of relations:

- Equivalence relations
- Partial orders

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

Classify the following:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \leq b\}$
- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a \equiv b \ (mod \ n)\}$
- $R(\Sigma^*) = \{(x, y) \mid x, y \in \Sigma^* \text{ and } x = \text{suff}(y)\}$
- $R(\mathbb{N}) = \{(a, b) \mid a \ (mod \ b) \neq 0\}$
- $R(\mathbb{R}) = \{(a, b) \mid a, b \in \mathbb{Z} \text{ and } a^2 \leq b^2\}$

CS 207 Discrete Mathematics – 2013-2014

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 7: Properties of equivalence relations and partial orders

August 08, 2013

Last time

Recap

- What are relaions?

Recap

- What are relaions?
- What are different types of relations?

Recap

- What are relaions?
- What are different types of relations?
  reflexive, transitive, symmetric, anti-symmetric

Recap

- What are relaions?
- What are different types of relations?
  reflexive, transitive, symmetric, anti-symmetric
- Equivalence relations and partial orders.

Recap

- What are relaions?
- What are different types of relations?
  reflexive, transitive, symmetric, anti-symmetric
- Equivalence relations and partial orders.

	reflexive	transitive	symmetric	anti-symmetric
equivalence relation	✓	✓	✓	
partial order	✓	✓		✓

- Representation of partial orders by graphs

Today

- Chains, anti-chains, properties of partial orders.

Today

- Chains, anti-chains, properties of partial orders.
- What are equivalence classes and properties of equivalence classes.

Posets, Chains and Anti-chians

Definition

A set S along with a relation $\preceq$, $(S, \preceq)$, is called a poset if $\preceq$ defines a partial order on S.

Posets, Chains and Anti-chians

Definition

A set S along with a relation $\preceq$, $(S, \preceq)$, is called a poset if $\preceq$ defines a partial order on S.

Definition

If $(S, \preceq)$ is a poset and every pair of elements in S is comparable, then $(S, \preceq)$ is called a totally ordered set.

Posets, Chains and Anti-chians

Definition

A set S along with a relation $\preceq$, $(S, \preceq)$, is called a poset if $\preceq$ defines a partial order on S.

Definition

If $(S, \preceq)$ is a poset and every pair of elements in S is comparable, then $(S, \preceq)$ is called a totally ordered set. A totally ordered set is called a *chain*.

Posets, Chains and Anti-chians

Definition

A set S along with a relation $\preceq$, $(S, \preceq)$, is called a poset if $\preceq$ defines a partial order on S.

Definition

If $(S, \preceq)$ is a poset and every pair of elements in S is comparable, then $(S, \preceq)$ is called a totally ordered set. A totally ordered set is called a *chain*.

Definition

Let $(S, \preceq)$ be a poset. A subset $A \subseteq S$ is called an anti-chain if no two elements of A are related to each other under $\preceq$.

Representing partial orders as directed graphs

What is a graph?

Representing partial orders as directed graphs

What is a graph?

Definition

A graph can be described by two sets: set V is called a set of vertices and set E is a subset of $V \times V$ and is called a set of edges, $G = (V, E)$.

Representing partial orders as directed graphs

What is a graph?

Definition

A graph can be described by two sets: set V is called a set of vertices and set E is a subset of $V \times V$ and is called a set of edges, $G = (V, E)$. Vertices $u, v \in V$ are said to be neighbours if $(u, v) \in E$.

Representing partial orders as directed graphs

What is a graph?

Definition

A graph can be described by two sets: set V is called a set of vertices and set E is a subset of $V \times V$ and is called a set of edges, $G = (V, E)$.
Vertices $u, v \in V$ are said to be neighbours if $(u, v) \in E$.
The graph is called directed if E is a set of ordered pairs.

What are the examples of graphs you may have seen:

Representing partial orders as directed graphs

What is a graph?

Definition

A graph can be described by two sets: set V is called a set of vertices and set E is a subset of $V \times V$ and is called a set of edges, $G = (V, E)$.
Vertices $u, v \in V$ are said to be neighbours if $(u, v) \in E$.
The graph is called directed if E is a set of ordered pairs.

What are the examples of graphs you may have seen:

- Social network graphs
- Tum-tum route graphs
- ...

Representing partial orders as directed graphs

Let $S = \{1, 2, 3\}$. Recall the poset $(\mathcal{P}(S), \subseteq)$.

Representing partial orders as directed graphs

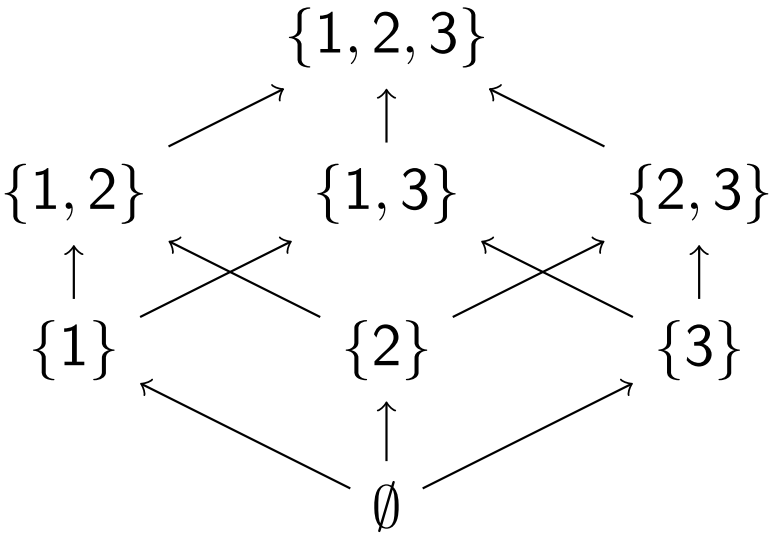
Let $S = \{1, 2, 3\}$. Recall the poset $(\mathcal{P}(S), \subseteq)$.
[CW] Describe $(\mathcal{P}(S), \subseteq)$.

Representing partial orders as directed graphs

Let $S = \{1, 2, 3\}$. Recall the poset $(\mathcal{P}(S), \subseteq)$.

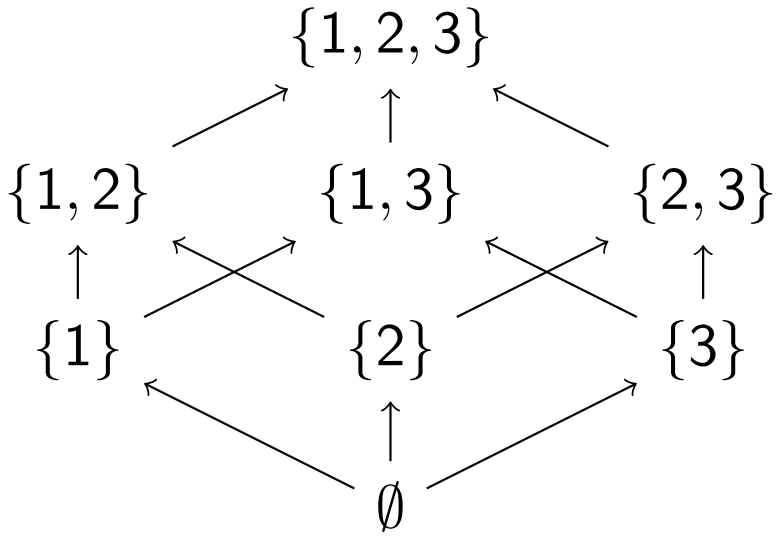
[CW] Describe $(\mathcal{P}(S), \subseteq)$.

A graph representing the poset:



Representing partial orders as directed graphs

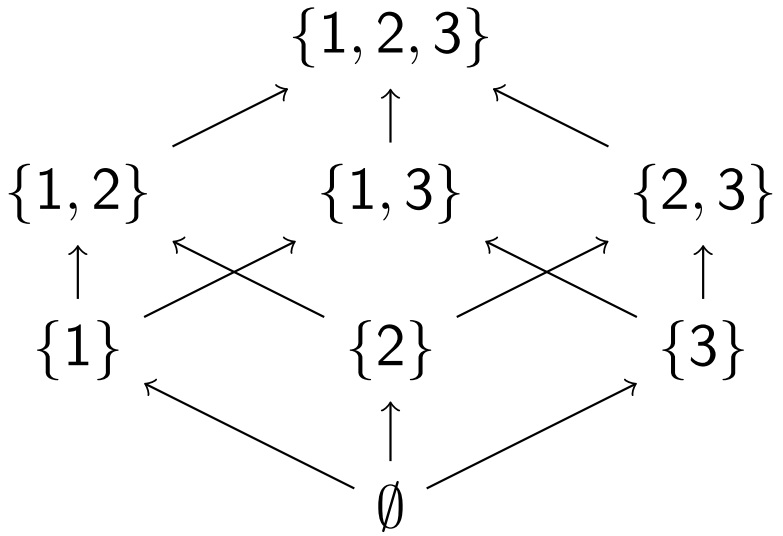
Let $S = \{1, 2, 3\}$. Recall the poset $(\mathcal{P}(S), \subseteq)$.
[CW] Describe $(\mathcal{P}(S), \subseteq)$.
A graph representing the poset:



[CW] What are the chains in this poset?

Representing partial orders as directed graphs

Let $S = \{1, 2, 3\}$. Recall the poset $(\mathcal{P}(S), \subseteq)$.
[CW] Describe $(\mathcal{P}(S), \subseteq)$.
A graph representing the poset:



[CW] What are the chains in this poset?
[CW] What are the anti-chains in this poset?

Chains and anti-chains

Theorem

If the largest chain in a poset $(S, \preceq)$ is of size m then S has at least m anti-chains.

Chains and anti-chains

Theorem

If the largest chain in a poset $(S, \preceq)$ is of size m then S has at least m anti-chains. The size of an anti-chain is the number of elements in the chain.

Chains and anti-chains

Theorem

If the largest chain in a poset $(S, \preceq)$ is of size m then S has at least m anti-chains.

Proof.

Let the chain be denoted as $a_1 \preceq a_2 \preceq \ldots \preceq a_m$. Now observe that every element of this chain, must go to different anti-chains.

Chains and anti-chains

Theorem

If the largest chain in a poset $(S, \preceq)$ is of size m then S has at least m anti-chains.

Proof.

Let the chain be denoted as $a_1 \preceq a_2 \preceq \ldots \preceq a_m$. Now observe that every element of this chain, must go to different anti-chains. Therefore, there are at least m anti-chains in $(S, \preceq)$. □

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

CS 207 Discrete Mathematics – 2013-2014

Nutan Limaye

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

Mathematical Reasoning and Mathematical Objects

Lecture 8: Properties of equivalence relations and partial orders

August 12, 2013

Last time

Recap

- What are graphs?

Recap

- What are graphs?
- Representation of partial orders by graphs.

Recap

- What are graphs?
- Representation of partial orders by graphs.
- Chains, anti-chains, properties of partial orders.

Recap

Definition

A set S along with a relation $\preceq$, $(S, \preceq)$, is called a poset if $\preceq$ defines a partial order on S.

Definition

If $(S, \preceq)$ is a poset and every pair of elements in S is comparable, then $(S, \preceq)$ is called a totally ordered set. A totally ordered set is called a *chain*.

Definition

Let $(S, \preceq)$ be a poset. A subset $A \subseteq S$ is called an anti-chain if no two (distinct) elements of A are related to each other under $\preceq$.

Recap

Theorem

If the largest chain in a poset $(S, \preceq)$ is of size m then S has at least m anti-chains.

Recap

Theorem

If the largest chain in a poset $(S, \preceq)$ is of size m then S has at least m anti-chains.

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Today

- Proof of Mirsky's theorem

Today

- Proof of Mirsky's theorem
- What are equivalence classes and properties of equivalence classes.

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.

[CW] For any $s \in S$, how large can $label(s)$ be?

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.
Let us now define sets $A_1, A_2, \ldots, A_m$ such that $A_i = \{x \mid label(x) = i\}$.

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.
Let us now define sets $A_1, A_2, \ldots, A_m$ such that $A_i = \{x \mid label(x) = i\}$.
It is easy to see that if $i \neq j$ then $A_i \cap A_j = \emptyset$. Also, it is easy to observe that $\cup_{i=1}^{m} A_i = S$.

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.
Let us now define sets $A_1, A_2, \ldots, A_m$ such that $A_i = \{x \mid label(x) = i\}$.
It is easy to see that if $i \neq j$ then $A_i \cap A_j = \emptyset$. Also, it is easy to observe that $\cup_{i=1}^{m} A_i = S$.
Now we prove that each A_i is an anti-chain. For $x, y \in A_i$ for some $i \in [m]$.

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.
Let us now define sets $A_1, A_2, \ldots, A_m$ such that $A_i = \{x \mid label(x) = i\}$.
It is easy to see that if $i \neq j$ then $A_i \cap A_j = \emptyset$. Also, it is easy to observe that $\cup_{i=1}^{m} A_i = S$.
Now we prove that each A_i is an anti-chain. For $x, y \in A_i$ for some $i \in [m]$. $[m] = \{1, 2, \ldots, m\}$

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.
Let us now define sets $A_1, A_2, \ldots, A_m$ such that $A_i = \{x \mid label(x) = i\}$.
It is easy to see that if $i \neq j$ then $A_i \cap A_j = \emptyset$. Also, it is easy to observe that $\cup_{i=1}^{m} A_i = S$.
Now we prove that each A_i is an anti-chain. For $x, y \in A_i$ for some $i \in [m]$. $\therefore label(x) = label(y) = i$. Suppose $x \preceq y$ then $label(x) < label(y)$. Contradiction!

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.
Let us now define sets $A_1, A_2, \ldots, A_m$ such that $A_i = \{x \mid label(x) = i\}$.
It is easy to see that if $i \neq j$ then $A_i \cap A_j = \emptyset$. Also, it is easy to observe that $\cup_{i=1}^{m} A_i = S$.
Now we prove that each A_i is an anti-chain. For $x, y \in A_i$ for some $i \in [m]$. $\therefore label(x) = label(y) = i$. Suppose $x \preceq y$ then $label(x) < label(y)$. Contradiction! Similarly, if $x \succeq y$ then we get a contradiction.

Chains and anti-chains

Theorem (Mirsky's theorem, 1971)

If the largest chain in a poset $(S, \preceq)$ is of size m then S can be partitioned into m anti-chains.

Proof.

For each element $s \in S$, let C_s be the set of all chains that have s as the maximum element. And define $label(s) := max_{c \in C_s} \{\text{size}(c)\}$.
Let us now define sets $A_1, A_2, \ldots, A_m$ such that $A_i = \{x \mid label(x) = i\}$.
It is easy to see that if $i \neq j$ then $A_i \cap A_j = \emptyset$. Also, it is easy to observe that $\cup_{i=1}^{m} A_i = S$.
Now we prove that each A_i is an anti-chain. For $x, y \in A_i$ for some $i \in [m]$. $\therefore label(x) = label(y) = i$. Suppose $x \preceq y$ then $label(x) < label(y)$. Contradiction! Similarly, if $x \succeq y$ then we get a contradiction. Hence, every A_i is an anti-chain.

□

Equivalence relations and equivalence classes

Definition

A relation R defined over a set A, denoted as $R(A)$ or (A, R), is called an equivalence relation if it is reflexive, transitive and symmetric.

Equivalence relations and equivalence classes

Definition

A relation R defined over a set A, denoted as $R(A)$ or (A, R), is called an equivalence relation if it is reflexive, transitive and symmetric.

Definition

Let $[x] := \{y \mid x, y \in A, \text{ and } (x, y) \in R\}$.
$[x]$ is called the equivalence class of x.

Example: Consider $(\mathbb{N}, \equiv (mod 4))$.

- $[0]$

Equivalence relations and equivalence classes

Definition

A relation R defined over a set A, denoted as $R(A)$ or (A, R), is called an equivalence relation if it is reflexive, transitive and symmetric.

Definition

Let $[x] := \{y \mid x, y \in A, \text{ and } (x, y) \in R\}$.
$[x]$ is called the equivalence class of x.

Example: Consider $(\mathbb{N}, \equiv (mod 4))$.

- $[0] = \{0, 4, 8, 12, 16, \ldots\}$

Equivalence relations and equivalence classes

Definition

A relation R defined over a set A, denoted as $R(A)$ or (A, R), is called an equivalence relation if it is reflexive, transitive and symmetric.

Definition

Let $[x] := \{y \mid x, y \in A, \text{ and } (x, y) \in R\}$.
$[x]$ is called the equivalence class of x.

Example: Consider $(\mathbb{N}, \equiv (mod 4))$.

- $[0] = \{0, 4, 8, 12, 16, \ldots\}$
- $[1]$

Equivalence relations and equivalence classes

Definition

A relation R defined over a set A, denoted as $R(A)$ or (A, R), is called an equivalence relation if it is reflexive, transitive and symmetric.

Definition

Let $[x] := \{y \mid x, y \in A, \text{ and } (x, y) \in R\}$.
$[x]$ is called the equivalence class of x.

Example: Consider $(\mathbb{N}, \equiv (mod 4))$.

- $[0] = \{0, 4, 8, 12, 16, \ldots\}$
- $[1] = \{1, 5, 9, 13, 17, \ldots\}$

Properties of equivalence relations

Let R be an equivalence relation of A. Let elements of A be x, y, z etc.

Lemma

The following three are equivalent: *(a)* xRy, *(b)* $[x] = [y]$, *(c)* $[x] \cap [y] \neq \emptyset$.

Properties of equivalence relations

Let R be an equivalence relation of A. Let elements of A be x, y, z etc.

Lemma

The following three are equivalent: *(a)* xRy, *(b)* $[x] = [y]$, *(c)* $[x] \cap [y] \neq \emptyset$.

Proof.

(a) $\Rightarrow$ (b): Say $z \in [x]$. But xRy. As xRy and R is symmetric, yRx. Therefore, yRx, xRz. R is transitive. Therefore, yRz, i.e. $z \in [y]$. This proves that $[x] \subseteq [y]$. The proof of $[y] \subseteq [x]$ is similar.

Properties of equivalence relations

Let R be an equivalence relation of A. Let elements of A be x, y, z etc.

Lemma

The following three are equivalent: *(a)* xRy, *(b)* $[x] = [y]$, *(c)* $[x] \cap [y] \neq \emptyset$.

Proof.

(a) $\Rightarrow$ (b): Say $z \in [x]$. But xRy. As xRy and R is symmetric, yRx. Therefore, yRx, xRz. R is transitive. Therefore, yRz, i.e. $z \in [y]$. This proves that $[x] \subseteq [y]$. The proof of $[y] \subseteq [x]$ is similar.
(b) $\Rightarrow$ (c): Say $[x] = [y]$. The only way $[x] \cap [y] = \emptyset$ is if $[x] = \emptyset$. However, as R is reflexive, $x \in [x] \neq \emptyset$.

Properties of equivalence relations

Let R be an equivalence relation of A. Let elements of A be x, y, z etc.

Lemma

The following three are equivalent: (a) xRy, (b) $[x] = [y]$, (c) $[x] \cap [y] \neq \emptyset$.

Proof.

(a) $\Rightarrow$ (b): Say $z \in [x]$. But xRy. As xRy and R is symmetric, yRx. Therefore, yRx, xRz. R is transitive. Therefore, yRz, i.e. $z \in [y]$. This proves that $[x] \subseteq [y]$. The proof of $[y] \subseteq [x]$ is similar.
(b) $\Rightarrow$ (c): Say $[x] = [y]$. The only way $[x] \cap [y] = \emptyset$ is if $[x] = \emptyset$. However, as R is reflexive, $x \in [x] \neq \emptyset$.
(c) $\Rightarrow$ (a): Let $z \in [x] \cap [y]$. Therefore, xRz and yRz. But as R is symmetric, zRy. But R is also transitive. Therefore xRz and zRy imply xRy. □

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*

Sets $X_1, X_2, \ldots, X_m$ are said to partition a set X if

- $\forall i, j \in \{1, 2, \ldots, m\}, i \neq j : X_i \cap X_j = \emptyset$
- $\forall x \in X, \exists i \in \{1, 2, \ldots, m\} : x \in X_i$

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*

Proof.

Let $[x] \neq [y]$ be two distinct equivalence classes of R. From the previous lemma $[x] \cap [y] = \emptyset$.

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*
- *Conversely, given a partition $\{A_i \mid i \in \{1, 2, \ldots, n\}\}$ of A, there is an equivalence relation R_A with equivalence classes $A_1, A_2, \ldots, A_n$.*

Proof.

Let $[x] \neq [y]$ be two distinct equivalence classes of R. From the previous lemma $[x] \cap [y] = \emptyset$. Also, for each $x \in A, x \in [x]$.

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*
- *Conversely, given a partition $\{A_i \mid i \in \{1, 2, \ldots, n\}\}$ of A, there is an equivalence relation R_A with equivalence classes $A_1, A_2, \ldots, A_n$.*

Proof.

Let $[x] \neq [y]$ be two distinct equivalence classes of R. From the previous lemma $[x] \cap [y] = \emptyset$. Also, for each $x \in A, x \in [x]$.

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*
- *Conversely, given a partition $\{A_i \mid i \in \{1, 2, \ldots, n\}\}$ of A, there is an equivalence relation R_A with equivalence classes $A_1, A_2, \ldots, A_n$.*

Proof.

Let $[x] \neq [y]$ be two distinct equivalence classes of R. From the previous lemma $[x] \cap [y] = \emptyset$. Also, for each $x \in A, x \in [x]$.

Let $R_A = \{(x, y) \mid \exists i : x, y \in A_i\}$.

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*
- *Conversely, given a partition $\{A_i \mid i \in \{1, 2, \ldots, n\}\}$ of A, there is an equivalence relation R_A with equivalence classes $A_1, A_2, \ldots, A_n$.*

Proof.

Let $[x] \neq [y]$ be two distinct equivalence classes of R. From the previous lemma $[x] \cap [y] = \emptyset$. Also, for each $x \in A, x \in [x]$.

Let $R_A = \{(x, y) \mid \exists i : x, y \in A_i\}$.
R_A relates (x, y) if they belong to the same part in the partition of A.

Equivalence classes and partitions

Theorem

Let R be an equivalence relation defined on a set A.

- *The equivalence classes of R, partition the set A.*
- *Conversely, given a partition $\{A_i \mid i \in \{1, 2, \ldots, n\}\}$ of A, there is an equivalence relation R_A with equivalence classes $A_1, A_2, \ldots, A_n$.*

Proof.

Let $[x] \neq [y]$ be two distinct equivalence classes of R. From the previous lemma $[x] \cap [y] = \emptyset$. Also, for each $x \in A, x \in [x]$.

Let $R_A = \{(x, y) \mid \exists i : x, y \in A_i\}$.
R_A is reflexive. If $(x, y) \in R_A$ then even $(y, x) \in R_A$. Finally, if $(x, y) \in R_A$ then $\exists i : x, y \in A_i$. Let that index be called i_0. Now if $(y, z) \in R_A$ then both y, z must be in the same part of the partition. But we know that $y \in A_{i_0}$. Therefore, $z \in A_{i_0}$. Hence, $x, z \in A_{i_0}$ and hence $(x, z) \in R_A$. This proves that R_A is also transitive. □