combra.cs.rutgers.edu

Notepad - Notepad - Notepad

206
Discrete Structures II

Konstantinos P. Michmizos

Computational Brain Lab

Computer Science | Rutgers University | NJ, USA

Lecture 4 | Proof – Proofs - Proofs | Tuesday 9/14 2021

Why I do not upload the slides before lectures

- I do not know how much of the planned lecture I will cover
  - But this would be easy to solve…
- Some of the slides, if given right upfront, are missing the mark (which is to make you THINK)
  - So, this is meant to keep you active (instead of passively absorbing the material…)
- But I upload the slides (+recording) right after the lecture!

Some more announcements

- Section 4 has ***in-person*** recitation on Tuesday 5:00 PM - 5:55 PM at Livingston TIL-254 (TA: Yuequn Zhang yuequn.zhang@rutgers.edu)
- Section 5 has ***in-person*** recitation on Thursday 3:00 PM - 3:55 PM at Livingston TIL-226 (TA: Vladimir Ivanov vai9@scarletmail.rutgers.edu)
- Section 6 has ***in-person*** recitation on Thursday 3:00 PM - 3:55 PM at Livingston LSH-B115 (TA: James Fu jf980@scarletmail.rutgers.edu)

Office hours for all TAs under home > course information > staff and office hours

Some more announcements

- ODS letter of accommodation: **Should (RE-)send that letter to their TAs and cc me**.
  - IF you do not do this, the TA has no way to know your name and you will not get any extra time. When you send the letter, please use **[CS 206 - ODS]**. Please make sure you send the email to the right TA. If your TA does not get the right email, from the right person, at the right time, we won't be able to do anything.

- Please note: EVEN if you have already sent such an email to me, and even if you have got a response back (in some cases, I have replied back), **you STILL have to send the letter to your TA.**

Reading for Quiz 1 (and beyond…)

Lecture 2	Recap and Basics of Counting	Chapters 1, 2 and 5 of Rosen
Lecture 3	Basics of Counting	Chapters 1, 2 and 5 of Rosen Chapter 15 of Lehman
Lecture 4+5+6+…	Basics of Counting	Chapters 6 of Rosen Chapter 15 of Lehman

What we will cover today

Combinatorics

- Recap
  - Functions – Proofs (Direct)
- Today
  - Proofs
    - Direct
    - Contrapositive
    - Case Analysis
    - Contradiction
    - Induction
  - Counting
    - Partition Method
    - Difference Method

Next Time

- Bijection Rule
- Product Rule

Course Outline

- Part I
  - Recap of basics – sets, function, proofs, induction
  - Basic counting techniques
  - Pigeonhole principle
  - Generating functions
- Part II
  - Sample spaces and events
  - Basics of probability
  - Independence, conditional probability
  - Random variables, expectation, variance
  - Moment generating functions
- Part III
  - Graph Theory
  - Machine learning and statistical inference

Functions

- What is a *function?*
  - A function *assigns* an element of one set to an element of another set
  - The **mapping** is done from one set, called *domain*, to another set, called *codomain*
  - Notation $f: A \mapsto B$
- Examples
  - $f: \mathbb{R} \mapsto \mathbb{R}$
  - $x \mapsto 4x^2$

  The familiar notation $f(a) = b$ indicates that f assigns the element $b \in B$ to a. Here b would be called the value of f at argument a
  - Example using a formula for b: $f(x) = 4x^2$

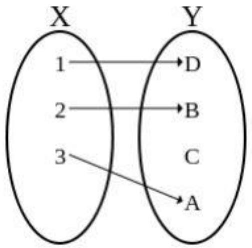
So far…

Types of Functions

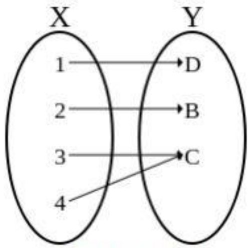
- Injection (one-to-one)
  - $f: X \mapsto Y$ is injective if each $x \in X$ is mapped to a *different* $y \in Y$.

  This function *preserves distinctness* as it never maps distinct elements of its domain to the same elements of its codomain.

- Subjection (onto)
  - $f: X \mapsto Y$ is subjective if each y $\in Y$, there exists $x \in X$ such that $f(x) = y$.

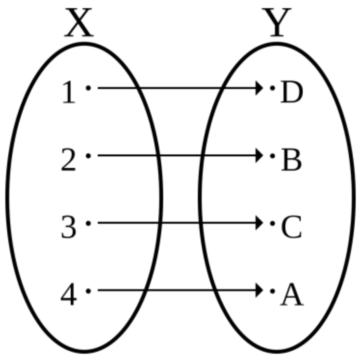


one-to-one (injective), but not onto



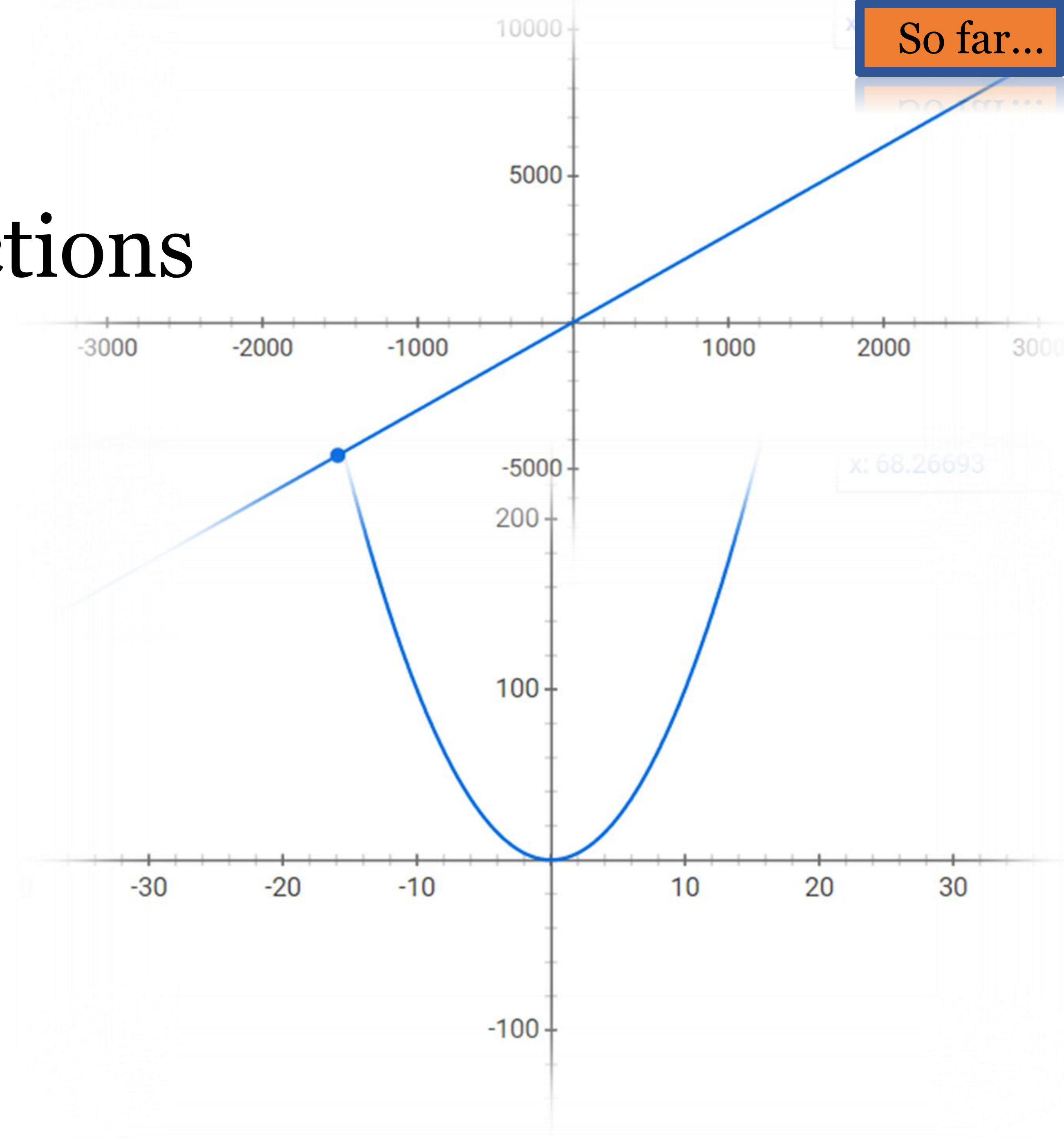
onto (surjective), but not one-to-one

- Bijection
  - $f: X \mapsto Y$ is a bijection if it is both one-to-one and onto.



So far...

Exercise 3: Types of Functions

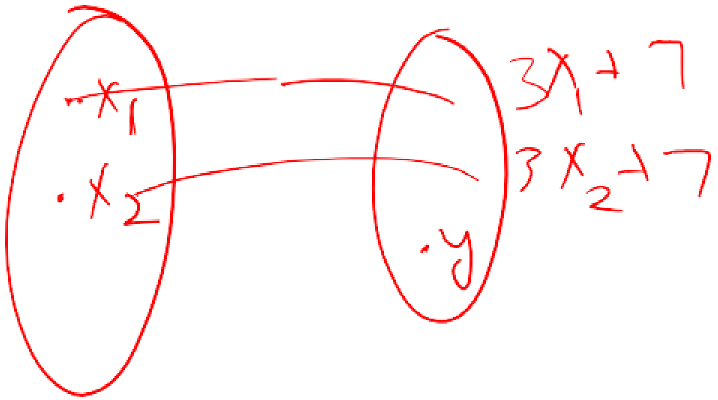


- $f: \mathbb{R} \mapsto \mathbb{R}, f(x) = 3x + 7$

- $f: \mathbb{R} \mapsto \mathbb{R}, f(x) = x^2$

Exercise 3: Types of Functions

- $f: \mathbb{R} \mapsto \mathbb{R}$, $f(x) = 3x + 7$



- $f(x) = 3x+7$ is one-to-one
  since if x_1 and x_2 are different then
  $3x_1+7$ and $3x_2+7$ are also different
- $f(x) = 3x+7$ is onto since for any real
  value y, $f\left(\frac{y-7}{3}\right) = y$

Hence $f(x) = 3x+7$ is a bijection

Exercise 3: Types of Functions

- $f: \mathbb{R} \mapsto \mathbb{R}, f(x) = x^2$

- $f(x) = x^2$ is not one-to-one since
  $f(2) = f(-2) = 4$

- $f(x) = x^2$ is not onto since for
  $y = -3$, no real value x exists such
  that $f(x) = -3$

Lehman, 3-15

So far...

Proofs

- A mathematical proof...
  - ...of a **proposition** is a chain of logical deductions from axioms and previously proved statements.
- Proposition
  - A statement that is either *true* or *false*
  - *e.g., Every even integer greater than 2 is the sum of two primes (Goldbach's Conjecture – remains unsolved since 1742...)*
- Predicates
  - A proposition whose truth depends on the value of variables
  - e.g., $P(n) ::= "n\ is\ a\ perfect\ square"$ – P(4) is true but P(5) is false

A ***prime*** is an integer greater than one that is not divisibl

by any other integer greater than 1, e.g., 2, 3, 5, 7, 11, . . .

So far...

Logical Deductions (or Inference Rules)

Used to prove new propositions using previously proved ones

- $\dfrac{P, P \Rightarrow Q}{Q}$
  - If P is true and P implies Q, then Q is true.
- $\dfrac{P \Rightarrow Q, Q \Rightarrow R}{P \Rightarrow R}$
  - If P implies Q and Q implies R, then P implies R.
- $\dfrac{\neg P \Rightarrow \neg Q}{Q \Rightarrow P}$
  - If $\neg P$ implies $\neg Q$, then Q implies P

If we can prove this ...

$$\frac{\boxed{\textit{antecedents}}}{\boxed{\textit{consequent}}}$$

...then this is true

So far...

Proving an Implication via Direct Proof

- To prove: $P \Rightarrow Q$
  - Assume that P is true.
  - Show that Q logically follows

and we stopped here...

Direct Proof

- To prove: $P \Rightarrow Q$
  - Assume that P is true.
  - Show that Q logically follows

The sum of two even numbers is even.

Proof $x = 2m, y = 2n$

$x+y = 2m+2n$

$= 2(m+n)$

The product of two odd numbers is odd.

Proof $x = 2m+1, y = 2n+1$

$xy = (2m+1)(2n+1)$

$= 4mn + 2m + 2n + 1$

$= 2(2mn+m+n) + 1$

New stuff...

Example of Proving an Implication

- Theorem: $\overset{P}{1 \leq x \leq 2} \Rightarrow \overset{Q}{x^2 - 3x + 2 \leq 0}$

Assume $1 \leq x \leq 2$

Step 1: $x^2 - 3x + 2 = (x-1)(x-2)$

Step 2: $1 \leq x \Rightarrow (x-1) \geq 0$

Step 3: $x \leq 2 \Rightarrow (x-2) \leq 0$

Step 4: $(x-1) \geq 0,\ (x-2) \leq 0 \Rightarrow (x-1)(x-2) \leq 0$

Intuition: When x grows, 3x grows faster than x^2 in that range.

Take a Break

5 min

New Stuff

What we will cover today

- Recap
  - ~~Sets – Venn – Functions – Proofs (Direct)~~
- Combinatorics
  - ~~Proofs~~
    - ~~Direct~~
    - Contrapositive
    - Case Analysis
    - Contradiction
    - Induction
  - Counting
    - Partition Method
    - Difference Method

proving “if P, then Q” is equivalent to proving “if not Q, then not P”

Proof by Contrapositive

- To prove: $P \Rightarrow Q$
  - **Goal**: Prove that $\neg Q \Rightarrow \neg P$.
  - **Method**: Assume ¬Q is true and show that $\neg P$ follows logically.

*i.e., we will **assume the opposite of our desired conclusion** and show that this fancy opposite conclusion could never be true in the first place.*

proving “if P, then Q” is equivalent to proving “if not Q, then not P”

Example of Proof by Contrapositive

- Theorem: *If r is irrational, then $\sqrt{r}$ is irrational.*

Rational Number

R is rational ⇔ there are integers a and b such that

$$\underbrace{r = \frac{a}{b}}$$

numerator

denominator

and b ≠ 0.

Remember:

1. A number is rational if it is equal to a ratio of integers

*2. The **sum** of two rational numbers is always a rational number*

*3. The **difference** of two rational numbers is always a rational number*

*4. The **product** of two rational numbers is always a rational number*

*5. The **quotient** of two rational numbers is always a rational number*

proving “if P, then Q” is equivalent to proving “if not Q, then not P”

Example of Proof by Contrapositive

- Theorem: *If r is irrational, then $\sqrt{r}$ is irrational.*

Proof:

We shall prove the contrapositive –

“if $\sqrt{r}$ is rational, then r is rational.”

Since $\sqrt{r}$ is rational, $\sqrt{r} = a/b$ for some integers a,b.

So $r = a^2/b^2$. Since a,b are integers, a^2,b^2 are integers.

Therefore, r is rational. Q.E.D.

(Q.E.D.) "which was to be demonstrated", or “quite easily done”. ☺

quod erat demonstrandum

Intuition: <u>Square roots</u> and <u>absolute values</u> are our worst enemies in proofs