combra.cs.rutgers.edu

Enjoy the last sunny days ☺

206
Discrete Structures II

Konstantinos P. Michmizos

Computational Brain Lab

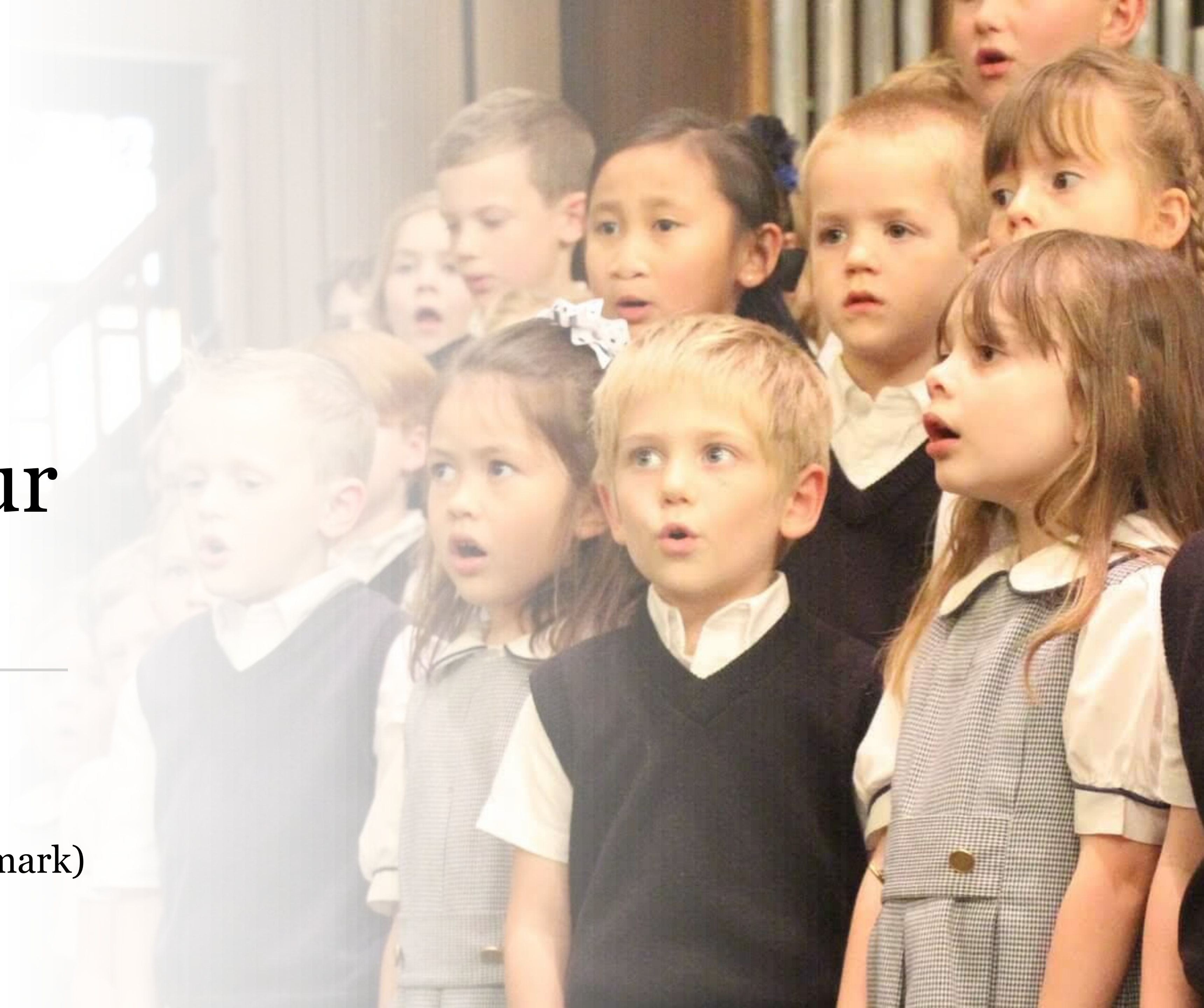
Computer Science | Rutgers University | NJ, USA

Lecture 5 | Proofs – Proofs - Proofs | Thursday February 1st 2021

How was your recitation?

Send me an email

(with a positive or negative remark)



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

What we will cover today

Combinatorics

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

Next Week

- 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

So far...

Proving an Implication via Direct Proof

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

So far...

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

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

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

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

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

So far...

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

Remember:

We start from P

and we construct Q

(while adhering to logic)

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

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

Proof by Contrapositive

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

Remember:

We reverse the direction

(double flip!)

*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.*

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: Square roots and absolute values are our worst enemies in proofs

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

Intuition: Square roots and absolute values are our worst enemies in proofs

Example of Proof by Case Analysis

- Theorem: *For all* $x \in \mathbb{R}, -5 \leq |x+2| - |x-3| \leq 5$

*We **hate** absolute values so we want to avoid them as soon as possible*

And we have two possible ways:-) (Squaring and…)

One of them is our goal here: To identify all possible cases

Example of Proof by Case Analysis

- Theorem: *For all* $x \in \mathbb{R}$, $-5 \leq |x+2| - |x-3| \leq 5$

$|x+2| = x+2$, if $x+2 \geq 0$ or $x \geq -2$

$|x+2| = -(x+2)$, if $x+2 < 0$ or $x < -2$

$|x-3| = x-3$ if $x \geq 3$

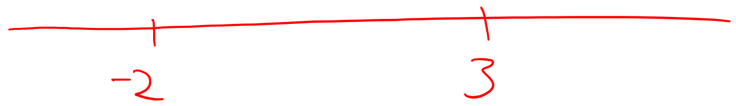
$|x-3| = -(x-3)$ if $x < 3$

$x < -2$ $-2 \leq x < 3$ $x \geq 3 \to$ Case I

Values of x Case III -2 Case II 3

Example of Proof by Case Analysis

- Theorem: *For all* $x \in \mathbb{R}, -5 \leq |x+2| - |x-3| \leq 5$



Case I: $x \geq 3$, Want $-5 \leq (x+2) - (x-3) \leq 5$

Want $-5 \leq 5 \leq 5$ $\square$

Case II: $-2 \leq x < 3$, Want $-5 \leq (x+2) - -(x-3) \leq 5$

Want $-5 \leq x+2+x-3 \leq 5$

Want $-5 \leq 2x-1 \leq 5$ $\square$

Case III $x < -2$, Want $-5 \leq -(x+2) - -(x-3) \leq 5$

Want $-5 \leq -(x+2) + x - 3 \leq 5$

Want $-5 \leq -5 \leq 5$ $\square$

Proof by Contradiction

Remember:

The main difference between

Proof by Contradiction and

Proof by Contrapositive is...

that there is no Q here!

$$\frac{\bar{P} \to \mathrm{F}}{P}$$

To prove P, you prove that **not P** would lead to a ridiculous result,

and ***so P must be true***.

I am working 20 hours per day.

If I had won the lottery, then I would not be working 20 hours per day.

$\therefore$ I have not won the lottery.

Proof by Contradiction – Work Chart

- To prove P
  - Assume P is false.
  - Logically deduce something that is known to be false.

Proof by Contradiction – Work Chart

To prove a proposition P by contradiction:

1. Write, “We use proof by contradiction.”

2. Write, “Suppose P is false.”

3. Deduce something known to be false (a logical contradiction).

4. Write, “This is a contradiction. Therefore, P must be true.”

Example of Proof by Contradiction

- Theorem: *There are infinitely many primes*

A **prime number** (or a prime) is a natural number greater than 1 that cannot be formed by multiplying two smaller natural numbers.

This is one of the most famous, most often quoted, and most beautiful proofs in all of mathematics. Its origins date back more than 2000 years to Euclid

Example of Proof by Contradiction

- Theorem: *There are infinitely many primes*

Assume: **There are finitely many primes** – And let p_1, p_2, …, p_N be all the primes.

Now we construct a new number, $p = p_1 p_2 \dots p_N + 1$

Clearly, *p* is larger than any of the primes, so it does not equal one of them.
Therefore it cannot be prime and must be **composite**, i.e., divisible by at least one of the primes.

But our assumption was that *p* is not prime and therefore divisible by any prime number.

On the other hand, we know that any number must be divisible by *some* prime (*fundamental theorem of arithmetic or the unique factorization theorem or the unique-prime-factorization theorem*)

This leads to a **contradiction**, and therefore the assumption must be false.

So there must be infinitely many primes.

Take a Break

5 min

Lehman, 115-129

Induction

- Let $P(m)$ be a predicate of non-negative integers

- You want to prove that $P(m)$ is true for all non-negative integers.

- Step 1: Prove that $P(0)$ is true

- Step 2: Prove that $P(n) \Rightarrow \mathrm{P(n+1)}$ for all non-negative integers.

Example of Induction

- Theorem: *For all* $n \in \mathbb{N}$,
  - $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

Example of Induction

- Theorem: *For all* $n \in \mathbb{N}$,
  - $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$

$P(n)$

<u>Base case</u>: $P(0)$ is true, for $n=0$
LHS $= 0$
RHS $= 0$

<u>Inductive Step</u>: $P(n) \Rightarrow P(n+1)$

Assume $P(n)$ is true. $1+2+\cdots+n = \frac{n(n+1)}{2}$

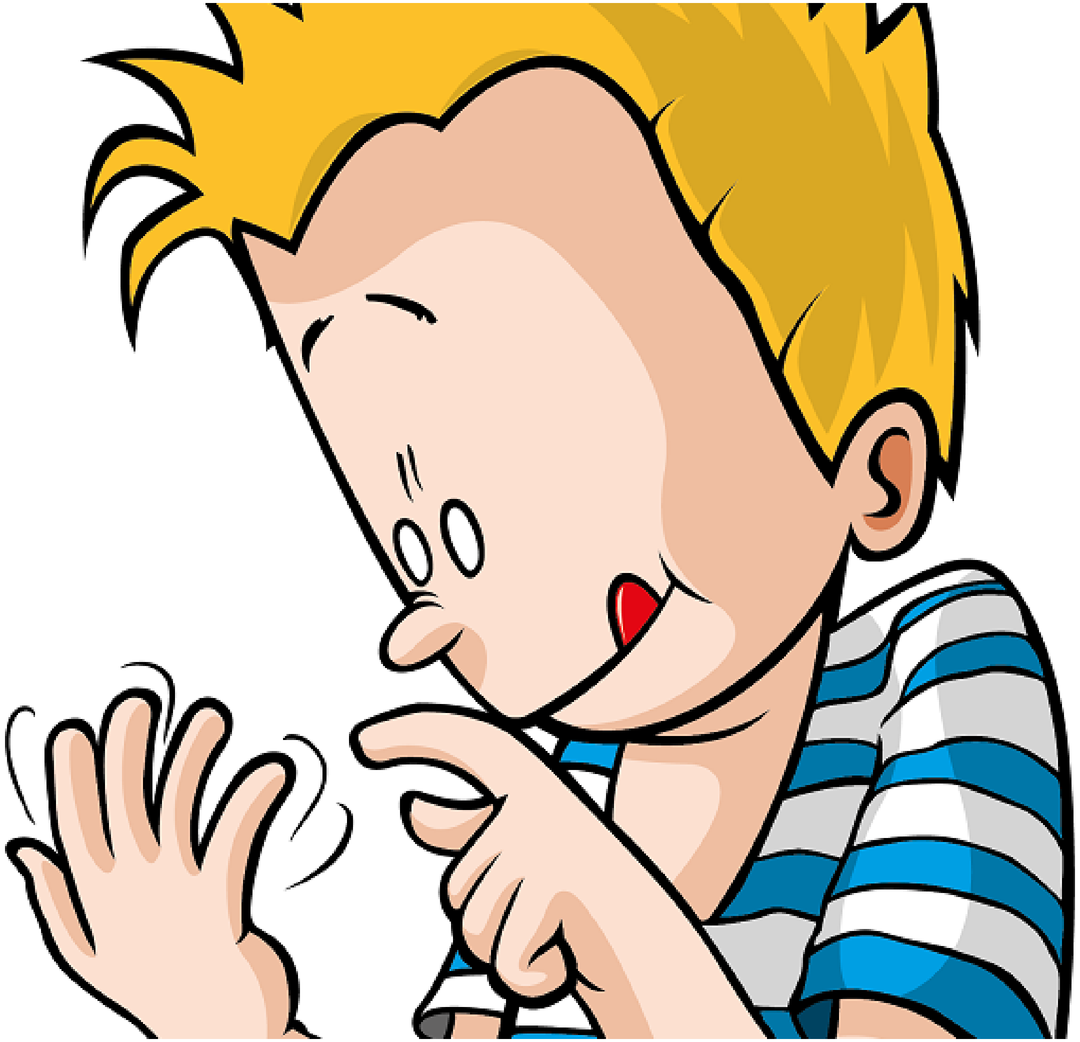
Want: $1+2+\cdots+n+n+1 = \frac{(n+1)(n+2)}{2}$

$1+2+\cdots+n+n+1 = \frac{n(n+1)}{2} + n+1 = \frac{(n+1)(n+2)}{2} = \text{RHS}$ $\square$

Intuition: During induction, my goal is to construct what I have assumed as true

New Stuff

Counting



Counting

- Basic Question: What is the size of a given set?

- Easy when the set is explicitly defined.
  - $X = \{1,2,3,4\}$, what is $|X|$?

- Tricky when set is implicit or a defined via set operations.
  - How many ways to get flush in the game of poker?
  - How many ways to assign time slots to courses at Rutgers?
  - How many operations before my algorithm terminates?

Counting

- In the next few lectures
  - Fundamental tools and techniques for counting
  - Sum Rule
  - Product Rule
  - Difference Method
  - Bijection Method
  - Permutations/Combinations
  - Inclusion Exclusion
  - Binomial/Multinomial coefficients

Fundamental Blocks

Intermediate

Advanced