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 | Proofs – Proofs - Proofs | Monday September 25th 2023

Quiz 1 – Next Week (during Recitation)

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	Basics of Counting	Chapters 6 of Rosen Chapter 15 of Lehman

What we will cover today

Combinatorics

- Recap
  - Sets - Venn – 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

So far...

Sets

- The order of elements is not significant, so $\{x, y\}$ and $\{y, x\}$ are the same set written two different ways.

- And what about $y = x$?
  - $\{x, x\} = \{x\}$

- The expression $e \in S$ asserts that e **is an element of** set S
  - E.g.,$32 \in S$ or $blue \notin S$

So far...

Sets - Set Operations

Example
$X ::= \{1,2,3\}$
$Y ::= \{2,3,4\}$

- Union: $X \cup Y$
  - All elements present in X or Y or both.
- Intersection: $X \cap Y$
  - All elements present in *both* X and Y.
- Difference: $X \setminus Y$
  - All elements present in X but not in Y.
  - Not symmetric!
- Product: $X \times Y$
  - Collection of all tuples (a, b) where $a \in X$ and $b \in Y$.
- Size: $|X|$
  - Number of elements in X.

$X \cup Y = \{1,2,3,4\}$

$X \cap Y = \{2,3\}$

$X \setminus Y = \{1\}$

$Y \setminus X = \{4\}$

$X \times Y = \{(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,2),(3,3),(3,4)\}$

$|X| = 3$

$|Y| = 3$

Power Set

$X = \{1,2,3\}$
$Power(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

- Let X be a set.
- $Power(X)$ = set of all subsets of X

- E.g., $Power(\{1,2\}) = \{1\}, \{2\}, and\ \{1,2\}$

- Is this correct?
  - NO!
  - $Power(\{1,2\}) = \{1\}, \{2\}, \{1,2\}, \boldsymbol{and}\ \{\}$

- Generally, if A has n elements, then there are 2^n sets in $Power(A)$

So far...

Set Builder Notation

- Often sets cannot be fully described by listing the elements explicitly or by taking unions, intersections, etc., of easily-described sets
- **Set builder notation** often comes to the rescue
- The idea is to define a set using a predicate; in particular, the set consists of all values that make the predicate true

Examples:

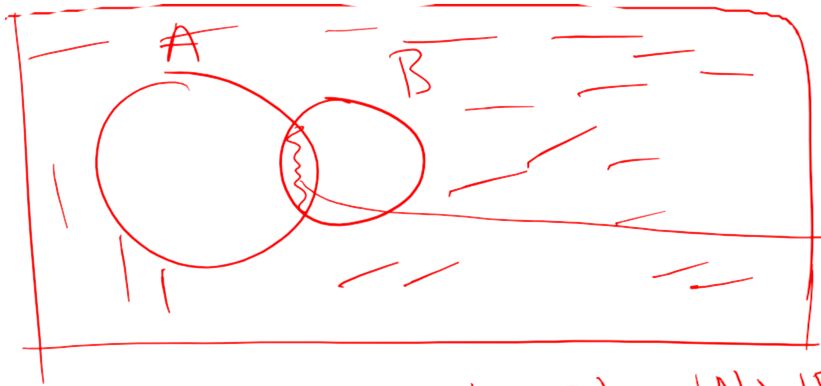
- $X = \{n \in \mathbb{N}: n \text{ is prime}\}$
- $Y = \{x \in \mathbb{R}: x^3 - 3x + 1 > 0\}$
- $Z = \{z \in YouTube\_videos: z \text{ is less than } 3 \text{ minutes long}\}$

So far...

Venn Diagram

- There are 131 students in CS 206.
- 100 like chocolate ice cream. 50 like vanilla ice cream.
- 20 like both chocolate and vanilla ice cream.
- Draw a Venn diagram to represent this.
- How many students do not like either flavor of ice cream.

A = chocolate
B = vanilla



$|A| = 100$
$|B| = 50$
$|A \cap B| = 20$

Want $131 - |A \cup B|$, $|A \cup B| = |A| + |B| - |A \cap B| = 130$

$\Rightarrow 131 - |A \cup B| = 1$

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: $f(x) = 4x^2$

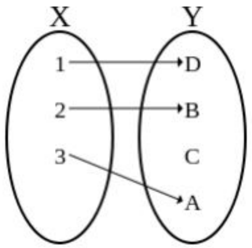
So far…

Types of Functions

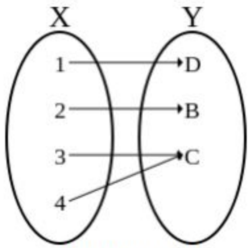
- Injection (one-to-one)
  - $f: X \mapsto Y$ is injective if each $x \in X$ is mapped to a *different* $y \in Y$.

  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 $f(x) = y$.

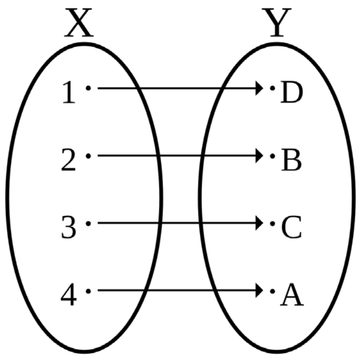


one-to-one (injective), but not onto



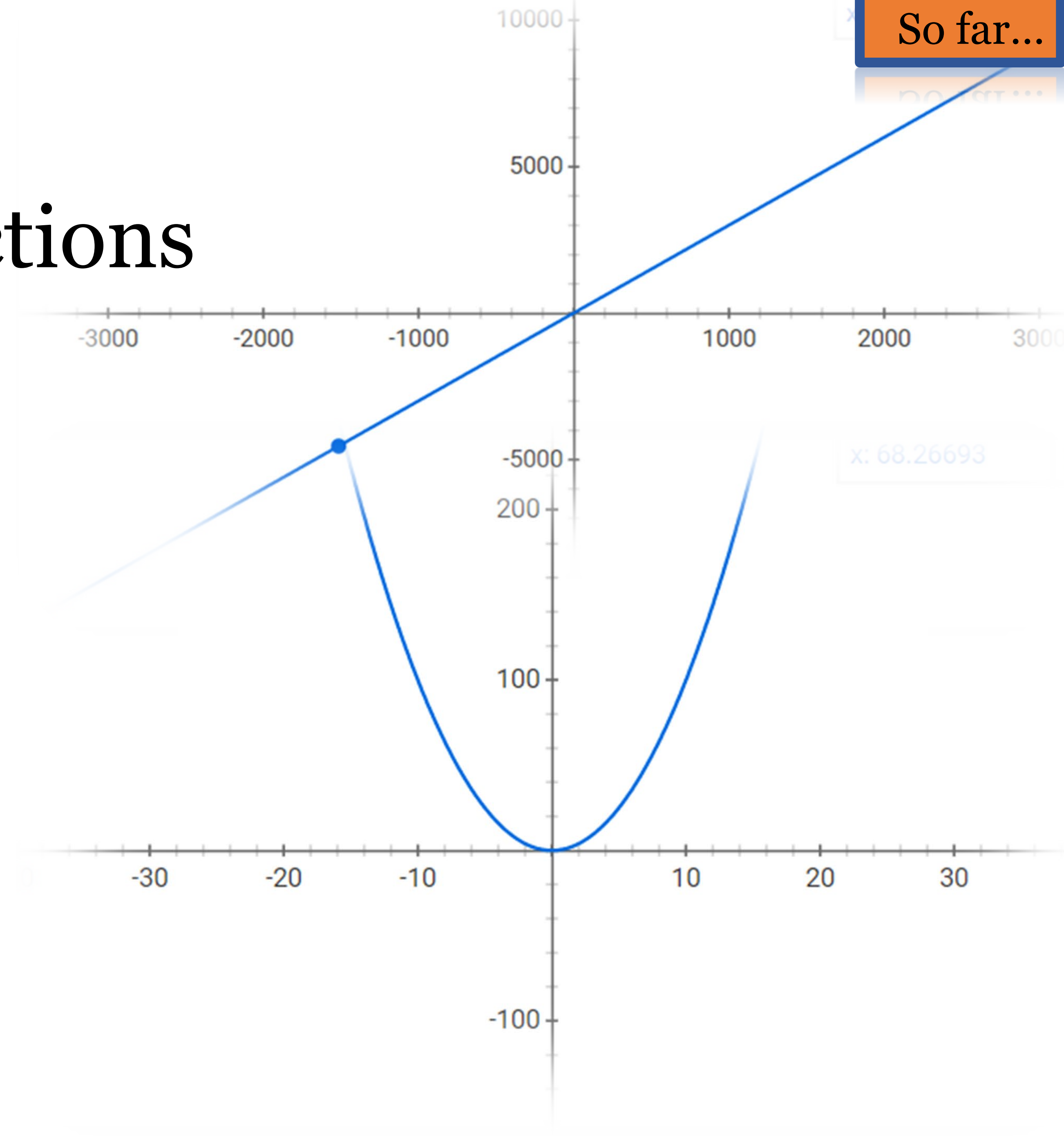
onto (surjective), but not one-to-one

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



So far...

Exercise 3: Types of Functions

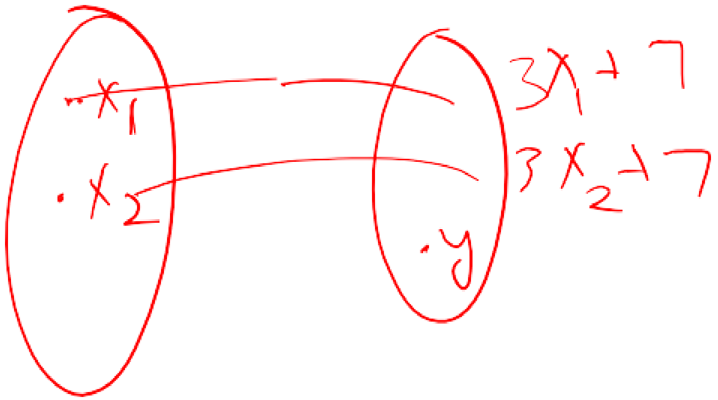


- $f: \mathbb{R} \mapsto \mathbb{R}, f(x) = 3x + 7$

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

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 $f(x) = -3$

Proofs

- A mathematical proof…
  - …of a **proposition** is a chain of logical deductions from axioms and previously proved statements.

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

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

- 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

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 …

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

…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

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

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

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

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

Example of Proving an Implication

P Q

- Theorem: $1 \leq x \leq 2 \Rightarrow x^2 - 3x + 2 \leq 0$

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.

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: $P \Rightarrow Q$
  - Prove that $\neg Q \Rightarrow \neg P$.
  - 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

numerator

$$r = \frac{a}{b}$$ and b ≠ 0.

denominator

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.

Why would we choose this method to solve this problem?

(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

What we will cover today

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

Example of Proof by Case Analysis

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

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

Two possible ways:-)

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

Example of Proof by Case Analysis

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

$|x+2| = x+2$, 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 $x < 3$

$x < -2 \qquad -2 \leq x < 3 \qquad x \geq 3 \rightarrow$ 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 $-5 \leq -5 \leq 5$ $\square$

What we will cover today

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

Proof by Contradiction

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

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 (Euclid)

- 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, $p = p_1 p_2 \ldots p_N + 1$

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.

Example of Proof by Contradiction (Euclid)

- Theorem: *There are infinitely many primes*

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

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

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.

Assume that my list of finite primes is {2, 3, 5, 7}

P = 2x3x5x7+1 = 211

211 is not divisible by either of 2, 3, 5, 7

211 could either be 1) a prime (**contradicts** with my assumption), or a) divisible by another prime that is not on the list above (**contradicts** with my assumption that I got the full list of primes)

Theorem: *There are infinitely many primes*

Theorem: *There are infinitely many primes*

- Suppose that $p_1=2 < p_2 = 3 < \ldots < p_r$ are all of the primes.
- Let $P = p_1p_2\ldots p_r+1$ and let p be a prime dividing P
- Then p cannot be any of $p_1, p_2, \ldots, p_r$, otherwise p would divide the difference $P\text{-}p_1p_2\ldots p_r = 1$, which is impossible.
- So this prime p is still another prime, and $p_1, p_2, \ldots, p_r$ would not be all of the primes.

It is a common mistake to think that this proof says the product $p_1p_2\ldots p_r+1$ is prime.

The proof actually only uses the fact that there is a prime dividing this product

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

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 $P(n) \Rightarrow \mathrm{P}(\mathrm{n}+1)$ 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: $1+2+\cdots n + n+1 = \frac{(n+1)(n+2)}{2}$

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

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