CS170: Discrete Methods in Computer Science
Summer 2023
Introduction

Instructor: Shaddin Dughmi[1]

[1] These slides adapt some content from similar slides by Aaron Cote.

Course Basics

- Instructor: Shaddin Dughmi (shaddin@)
- TAs: Chandra Mukherjee (cmukherj@) and Neel Patel (neelbpat@)
- CPs: Ramiro Deo-Campo Vong (rdeocamp@usc), David Lee (dhlee@), Aditya Prasad (aprasad4@)
- Office Hours: TBD
- Lecture: MWF 2:00-4:05 pm in GFS 118
- Discussion: Thursday 2:00-4:05pm in GFS 118
- Course duration: 6 weeks
- Book: Essential Discrete Mathematics by Lewis and Zax
- Website (forthcoming): https://viterbi-web.usc.edu/ shaddin/cs170su23

Requirements and Grading

- 4-5 homeworks, worth 50%
  - No late homework allowed, but will discount lowest hw score by half
- Midterm worth 20% (Thursday Jul 20, during discussion section)
- Final worth 30% (Week of August 8, TBD).

What is this course about?

- Discrete Math: disconnected, non-smooth objects (booleans, integers, graphs, etc)
  - Most relevant to computer science and algorithms
  - Quite different from continous math like calculus
- Logic and proofs
  - Reason clearly and precisely by using logic, instead of relying exclusivly on fallible intuition
  - Proof: Argument which starts from assumptions (a.k.a. axioms), applies rules of logic clearly in stepwise fashion, to establish a conclusion

Outline

1. Generalization
2. Mathematical Primitives and Notation
3. Some Examples of Proofs

Characterizing Triangles

- Is there a triangle with sides of length 2,3,6? What about 2,3,4?

Characterizing Triangles

- Is there a triangle with sides of length 2,3,6? What about 2,3,4?
- Is there a general rule to determine whether a triangle of given side lengths exists?

Characterizing Triangles

- Is there a triangle with sides of length 2,3,6? What about 2,3,4?
- Is there a general rule to determine whether a triangle of given side lengths exists?

Given three nonnegative numbers x, y, z with $x \leq y \leq z$, there is a triangle with side lengths x, y, z if and only if $z \leq x + y$.

The "only if" part of this statement is often called the Triangle Inequality

Pigeonhole Principle

- In a group of 8 people, two of them must have been born on the same day of the week.

Pigeonhole Principle

- In a group of 8 people, two of them must have been born on the same day of the week.
- What about 14 people? 15 people?

Pigeonhole Principle

- In a group of 8 people, two of them must have been born on the same day of the week.
- What about 14 people? 15 people?
- If 11 pigeons go into 10 holes, there must be a hole with two pigeons.

Pigeonhole Principle

- In a group of 8 people, two of them must have been born on the same day of the week.
- What about 14 people? 15 people?
- If 11 pigeons go into 10 holes, there must be a hole with two pigeons.
- What about 170 pigeons and 169 holes? 85 holes? 84 holes?

Pigeonhole Principle

- In a group of 8 people, two of them must have been born on the same day of the week.
- What about 14 people? 15 people?
- If 11 pigeons go into 10 holes, there must be a hole with two pigeons.
- What about 170 pigeons and 169 holes? 85 holes? 84 holes?
- Is there a general principle here?

Pigeonhole Principle

Pigeonhole Principle (colloquial)

If m pigeons go into n holes, and $m > n$, then there is a hole with two pigeons.

Pigeonhole Principle

Pigeonhole Principle (colloquial)

If m pigeons go into n holes, and $m > n$, then there is a hole with two pigeons.

Pigeonhole Principle

If $f : X \to Y$ and $|X| > |Y|$, then there are $x_1, x_2 \in X$ with $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$.

Pigeonhole Principle

Pigeonhole Principle (colloquial)

If m pigeons go into n holes, and $m > n$, then there is a hole with two pigeons.

Pigeonhole Principle

If $f : X \to Y$ and $|X| > |Y|$, then there are $x_1, x_2 \in X$ with $x_1 \neq x_2$ such that $f(x_1) = f(x_2)$.

Extended Pigeonhole Principle

If $f : X \to Y$ and $|X| > k|Y|$ for a positive integer k, then there are distinct $x_1, x_2, \ldots x_{k+1} \in X$ such that $f(x_1) = f(x_2) = \ldots = f(x_{k+1})$.

i.e., if there are more than k times as many pigeons as holes, then there is a hole with $k + 1$ pigeons.

Fundamental Theorem of Arithmetic

- Prime number: An integer greater than 1 which is divisible only by itself and 1.
  - 2,3,5,7,11,17,...
- Write down the following numbers as a product of primes in nondecreasing order: 15,18,60,61,62

Fundamental Theorem of Arithmetic

- Prime number: An integer greater than 1 which is divisible only by itself and 1.
  - 2,3,5,7,11,17,...
- Write down the following numbers as a product of primes in nondecreasing order: 15,18,60,61,62

Prime factorization of integer n

$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, where $p_1 < p_2 < \ldots < p_k$ are primes, and $e_1, \ldots, e_k$ are positive integers.

Fundamental Theorem of Arithmetic

- Prime number: An integer greater than 1 which is divisible only by itself and 1.
  - 2,3,5,7,11,17,...
- Write down the following numbers as a product of primes in nondecreasing order: 15,18,60,61,62

Prime factorization of integer n

$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$, where $p_1 < p_2 < \ldots < p_k$ are primes, and $e_1, \ldots, e_k$ are positive integers.

Fundamental Theorem of Arithmetic

Every integer $n > 1$ has one and only one prime factorization.

Generalization

We just saw three illustrations of generalization: From a few examples, we extrapolated a principle or statement which applies more broadly.

- Useful in more situations
- Saves you from redoing the work every time
- Helps you understand what's really going on
- Strips away irrelevant details and uncovers the common pattern / phenomenon

Outline

Sets

A set is a collection of things (or elements), which are called its members.

- Common to denote a set with uppercase, elements in lowercase.
- When describing a set explicitly by listing its members, we use curly braces
  - E.g. $A = \{1, 2, 3\}$.
- $x \in X$ means that x is a member of set X.
- $x \notin X$ means that x is not a member of X
- Repetition does not matter, so can think of members as distinct (i.e., different)
- Order does not matter
- $|X|$ is the size (a.k.a. cardinality) of set X
- A set may be finite (e.g. days of the week) or infinite (e.g. the integers, real numbers, computer programs).

Functions

A function f is a rule which associates each member of one set X with exactly one member of another set Y.

- We write $f : X \to Y$, and say f maps elements of the set X to elements of the set Y.
- If f associates $x \in X$ with $y \in Y$, we write $y = f(x)$. We call x the argument or input of f, and y the value or output
- Each $x \in X$ gets mapped to exactly one $y \in Y$
- Each $y \in Y$ may have one $x \in X$ that maps to it, or many, or none.

We will get into more detail on sets and functions later in the class.

Outline

For positive integers a, b, we use $a|b$ to denote that a divides b evenly. We also say a is a factor (or divisor) of b.

Claim

If p, m, n are positive integers, p is prime, and $p|mn$, then $p|m$ or $p|n$.

For positive integers a, b, we use $a|b$ to denote that a divides b evenly. We also say a is a factor (or divisor) of b.

Claim

If p, m, n are positive integers, p is prime, and $p|mn$, then $p|m$ or $p|n$.

- p appears in the prime factorization of mn.
- The (unique) prime factorization of mn can be obtained by combining the prime factorizations of m and n.
- p must have appeared in the prime factorization of m or n (or both)

Extended Pigeonhole Principle

If $f : X \to Y$ and $|X| > k|Y|$ for a positive integer k, then there are distinct $x_1, x_2, \ldots x_{k+1} \in X$ such that $f(x_1) = f(x_2) = \ldots = f(x_{k+1})$.

i.e., If m pigeons go into n holes, and $m > kn$, then there is a hole with $k + 1$ pigeons.

Extended Pigeonhole Principle

If $f : X \to Y$ and $|X| > k|Y|$ for a positive integer k, then there are distinct $x_1, x_2, \ldots x_{k+1} \in X$ such that $f(x_1) = f(x_2) = \ldots = f(x_{k+1})$.

i.e., If m pigeons go into n holes, and $m > kn$, then there is a hole with $k+1$ pigeons.

- Is it possible that each hole has at most k pigeons?
- If that were the case, then there are at most kn pigeons overall
- But the number of pigeons m is strictly greater than kn, so this can't be.

Extended Pigeonhole Principle

If $f : X \to Y$ and $|X| > k|Y|$ for a positive integer k, then there are distinct $x_1, x_2, \ldots x_{k+1} \in X$ such that $f(x_1) = f(x_2) = \ldots = f(x_{k+1})$.

i.e., If m pigeons go into n holes, and $m > kn$, then there is a hole with $k + 1$ pigeons.

- Is it possible that each hole has at most k pigeons?
- If that were the case, then there are at most kn pigeons overall
- But the number of pigeons m is strictly greater than kn, so this can't be.

This is called a proof by contradiction.

Claim

Given any $m \geq 13$ distinct integers between 2 and 40, at least two of them must have a common divisor greater than 1.

Claim

Given any $m \geq 13$ distinct integers between 2 and 40, at least two of them must have a common divisor greater than 1.

- Take each of the given $m > 13$ integers and map it to one of its prime divisors arbitrarily.
- Only 12 primes are relevant here, since there are 12 primes under 40: 2,3,5,7,11,13,17,19,23,29,31,37
- By the pigeonhole principle, two of the given m integers must map to the same prime. Therefore, they have a common divisor.

Claim

There are arbitrarily large primes.

Claim

There are arbitrarily large primes.

- Take any prime p
- $p!$ is divisible by all primes less than or equal to p
- $p! + 1$ is not divisible by any prime less than or equal to p (remainder is 1)
- By fundamental theorem of arithmetic, $p! + 1$ has a prime divisor that is bigger than p (possibly itself).
- So for any prime p, we were able to show that there is a bigger one.

A number is rational if it can be written as $\frac{a}{b}$, where a and b are integers. Otherwise, we call it irrational.

Claim

$\sqrt{2}$ is irrational.

A number is rational if it can be written as $\frac{a}{b}$, where a and b are integers. Otherwise, we call it irrational.

Claim

$\sqrt{2}$ is irrational.

- Suppose for a contradiction that $\sqrt{2}$ is rational.
- There are a, b with $\frac{a}{b} = \sqrt{2}$. Take such a and b with no common divisors (i.e. cancel out the common prime divisors).
- $a^2 = 2b^2$
- $2|a$, and therefore $a = 2k$ for some integer k
- $b^2 = \frac{a^2}{2} = \frac{4k^2}{2} = 2k^2$
- $2|b^2$, and therefore $2|b$.
- But we took a and b with no common divisors, a contradiction!

Claim

There exist two irrational numbers x, y, such that x^y is rational.

Claim

There exist two irrational numbers x, y, such that x^y is rational.

- We already know $\sqrt{2}$ is irrational.
- Consider $\sqrt{2}^{\sqrt{2}}$. Either this is rational or it is not.
- If it is rational, we can take $x = y = \sqrt{2}$.
- If it is irrational, then take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, both irrational.
  $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$, a rational!

Claim

There exist two irrational numbers x, y, such that x^y is rational.

- We already know $\sqrt{2}$ is irrational.
- Consider $\sqrt{2}^{\sqrt{2}}$. Either this is rational or it is not.
- If it is rational, we can take $x = y = \sqrt{2}$.
- If it is irrational, then take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$, both irrational.
  $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$, a rational!

Note

We proved such x, y exist without identifying them! This sort of existence proof is called “nonconstructive”.