CMSC 250: Discrete Structures

Omkar Pathak*

January 21, 2023

These are my notes for UMD's CMSC 250, which covers "fundamental mathematical topics related to computer science." The notes start from the third week of the class (September 13, 2022), as I added the class after the second week of classes. This course is taught by Prof. Mohammed Nayeem Teli.

Contents

*Email: omkarp07.terpmail.umd.edu

§1 Tuesday, September 13, 2022

§1.1 Predicates

Definition 1.1. A **predicate** is a statement or mathematical assertion that contains variables, which are sometimes referred to as predicate variables. Predicates do not have truth values that can be easily detected; they are not **propositions**. As a result, we cannot use propositional logic to draw conclusions.

Definition 1.2. A **premise** is a proposition used as evidence in an argument.

Example 1.3

The sentence "x is greater than 3" has two parts: the variable x is the **subject**, and the part "greater than 3" is the **predicate**.

§1.2 Quantifiers

Definition 1.4. The **universal quantifier**, $\forall$, says that a statement must be true for **all** values of a variable.

Example 1.5

Below are some examples of the universal quantifier:

- $\forall x$, $\text{Human}(x) \to \text{Mortal}(x)$
- $\forall x$, $x > 0 \to x + 1 > 0$

Here are some more examples of the universal quantifier. To make the universe of values explicit, we use set membership notation ($\in$):

Example 1.6

$\forall x \in \mathbb{Z}, x > 0 \to x + 1 > 0 \equiv \forall x : (x \in \mathbb{Z} \land x > 0) \to x + 1 > 0$

Definition 1.7. The **existential quantifier**, $\exists$, says that a statement must eb true for at least one value of the variable.

Example 1.8

There is a student in CMSC 250. $\exists x \in P$ such that x is a student in CMSC 250, where P is the set of all people.

Note 1.9. Quantifiers have higher precedence than logical values (e.g. if we have $\forall P(x), Q(x)$, the $\forall$ quantifier has higher precedence than the implication (or a biconditional, and/or statements, etc.).

Theorem 1.10 (DeMorgan's Laws, quantifier edition)
The following equivalencies hold:

- $\neg\forall x : P(x) \equiv \exists x : \neg P(x)$
- $\neg\exists x : P(x) \equiv \forall x : \neg P(x)$

§2 Thursday, September 15, 2022

§2.1 Nested Quantifiers

We can **nest** quantifiers as follows:

Example 2.1
Nesting quantifiers:

- $\forall x \forall y, P(x, y)$
- $\forall y, \forall x, P(x, y)$
- $\exists x, \forall y, P(x, y)$
- $\forall y, \exists x, P(x, y)$
- $\exists x, \exists y, P(x, y)$

We can also negate these quantifiers accordingly. Note that when nesting quantifier, the **domain** of the variables that the quantifiers operate on matter. Take a look at the next example:

Example 2.2
Is the following true?

$$\forall x, \exists y : y < x$$

Solution. We cannot answer this question without knowing the sets of numbers in which x and y are in. □

§2.2 Negations

How can we negate statements with quantifiers?

Example 2.3
All cats are furry.

Solution. This is left as an exercise. □

Example 2.4
Some snowflakes are the same.

Solution. This is left as an exercise. □

§3 Tuesday, September 20, 2022

§3.1 Quantifier Rules of Inference

§3.1.1 Universal Instantiation

Definition 3.1. We conclude that $P(c)$ is true, where c is a particular member of the domain, given the premise $\forall x P(x)$ is true.

$$\forall x \in D, P(x)$$
$$\therefore P(c), \text{ for any } c \in D$$

§3.1.2 Universal Generalization

Definition 3.2. We have $\forall x\ P(x)$, given the premise that $P(c)$ is true for all elements c in the domain. The element c must be an arbitrary, and not a specific element of the domain.

$$P(c), \text{ for any arbitrary } c \in D$$
$$\therefore \forall x \in D,\ P(x)$$

§3.1.3 Existential Instantiation

Definition 3.3. If we know $\exists x P(x)$ is true, we can conclude there is an element c in the domain for which $P(c)$ is true. In other words, we have

$$\exists x \in D \text{ s.t. } P(x)$$
$$\therefore P(c) \text{ for some element } c$$

§3.1.4 Existential Generalization

For a particular element c, if we know $P(c)$ is true, we can conclude that $\exists x P(x)$ is true.

$$P(c) \text{ for some } c \in D$$
$$\therefore \exists x \in D \text{ s.t. } P(x)$$

§3.2 Methods of proof

We have now reached a point at which we can begin discussing different methods of proof (we will define what a proof is shortly). Below are some definitions of terms that we will use in proofs:

Definition 3.4.

- A **theorem** is a statement that can be shown to be true.
- A **lemma** is a less important theorem that is helpful in the proof of other results.
- A **corollary** is a theorem that can be established directly from a theorem that can be proved.
- A **conjecture** is a statement that is being proposed to being a true statement.
- A **proof** is a valid argument that establishes the truth of a theorem
- An **axiom** is a statement we assume to be true

§3.2.1 Tips to write proofs

A good proof should have:

- A clear statement of what is to prove (a theorem, lemma, corollary, lemma, proposition, etc.)
- The word "proof" to indicate where the proof starts
- A clear indication of flow
- A clear justification for each step
- A clear indication for each step
- A clear indication for the conclusion
- The abbreviation "QED" ("Quod Erat Demonstradum") or "that which was to be proved") or equivalent (i.e. a square box) to indicate the end of the proof

§3.2.2 Summary of proof methods

- Direct proof
- Proof by contrapositive
- Proof by contradiction
- Exhaustive proof
- Proof by induction

- Proof by casework

Note that exhaustive proof is when one checks each case and either proves or disproves each case. Today, we'll go over examples of direct proof and proof by contrapositive. Before that, we'll go over some basic number definitions.

§3.2.3 Number definitions

Definition 3.5. An integer n is **even** if $n = 2k$ for some integer k¡ and is **odd** if$n = 2k + 1$ for some integer k.

Definition 3.6. A number q is **rational** if there exist integers a, b, $b \neq 0$, such that $q = \frac{a}{b}$ and where a and b have no common factors besides 1 and -1.

Definition 3.7. A real number that is not rational is **irrational**.

§3.2.4 Closure

- $\mathbb{Z}$ is closed under addition
- $\mathbb{Q}^{\neq 0}$ is closed under division (nonzero rationals are closed under division)
- $\mathbb{Z}^{\neq 0}$ is closed under division (nonzero integers are closed under division)

§3.2.5 Direct proof examples

Example 3.8

Prove square of an even number is even.

Proof. We have $P(x) : (x \text{ is even})$, and want to prove $\forall x\ Q(x) : (x^2 \text{ is even})$. Suppose $x = 2k$, where $k \in \mathbb{Z}$, by the definition of even numbers. We will proceed with direct proof, which will involve taking a series of logical steps to reach the conclusion directly from the hypothesis. Now, we have $x^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2)$. Let $y = 2k^2$. We have $y \in \mathbb{Z}$ because integers are closed under multiplication. Thus, $x^2 = 2y$. By the definition of even numbers, we have that x is even. QED. □

Example 3.9

The product of two odd numbers is odd.

Proof. Suppose we have $x = 2k + 1$ and $y = 2l + 1$. We have $P(a) : (a \text{ is odd})$, is true for x and y. We want to prove that $\forall x, y, z \in \mathbb{Z}, (P(x) \cdot P(y)) = z \rightarrow P(z))$. We will proceed with a direct proof.

Let $x = 2k + 1$, $y = 2l + 1$, for $k, l \in \mathbb{Z}$. Then, we have $x \cdot y = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1$. Note that $4kl$, $2k$, and $2l$ are even, by the definition of even numbers. Therefore, we have that $(4kl + 2k + 2l) + 1 = 2(2kl + k + l) + 1 = 2m + 1$ ($m = 2kl + k + 1$ is an integer, because integers are closed under multiplication and addition) is odd, by the definition of odd numbers. QED.

□

Example 3.10

The sum of two rational numbers is rational.

Proof. Suppose we have $q = \frac{a}{b}$ and $r = \frac{c}{d}$, where $a, b, c, d \in \mathbb{Z}$, and $b, d \neq 0$. We have $P(k) : (k \text{ is rational})$ is true for q and r. We want to prove that $\forall q, r, s \in \mathbb{Q}$, $(P(q) + P(r) = s \to P(s))$. We will proceed with a direct proof.

Let's add p and q. We get $\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}$. Now, because integers are closed under multiplication and addition, we have that $ad + bc = m$ and $bd = n$ are both integers. As a result, we have $p + q = \frac{m}{n}$, where both m and n are integers. Note that n is not 0 (we have to show this!) because n is the result of the product of two nonzero integers, which is always nonzero. Therefore, $p + q$ is also an integer. QED. □

§3.2.6 Proof by contrapositive examples

Example 3.11

If $3n + 2$ is odd, where n is an integer, then n is odd.

Proof. Note that the above statement is logically equivalent to "If n is even, then $3n + 2$ is even, where n is an integer." We can prove either statement. We will proceed with a proof by contraposition.

Suppose we have $n = 2k$, where $k \in \mathbb{Z}$. Then, $3n + 2 = 3(2k) + 2 = 2(3k) + 2$. Let $y = 3k$. Then, we have $3n + 2 = 2y + 2 = 2(y + 1)$. If we let $m = y + 1$, we have $3n + 2 = 2m$, meaning $3n + 2$ is even, and proving the contrapositive of this statement. Hence, we have that if $3n + 2$ is odd, where n is an integer, then n is odd. QED. □

§4 Thursday, September 22, 2022

Let's continue with some examples of proof by contraposition.

Example 4.1

If n^2 is even, then n is even.

Proof. This is left as an exercise. Take the contrapositive of the statement, e.g. "If n is odd, then n^2 is odd." and prove this. Let $n = 2k + 1$, where $k \in \mathbb{Z}$, compute n^2, prove that this is odd, and ensure that you state that the contrapositive is logically equivalent to the original statement. □

Example 4.2

If $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ and $b \leq \sqrt{n}$.

Proof. Take the contrapositive "If $a > \sqrt{n}$ and $b > \sqrt{n}$, $n \neq ab$. If $a > \sqrt{n}$ and $b > \sqrt{n}$, we have $a \cdot b > \sqrt{n} \cdot \sqrt{n}$, e.g. $ab > n$. Because $ab > n$, we have $n \neq ab$, proving the contrapositive of the original statement, and therefore proving the original statement. □

§4.1 More proof examples

§4.1.1 Proof by contradiction examples

Example 4.3

At least four of any 22 days must fall on the same day of the week.

Proof. Assume at most 3 days of any 22 days fall on the same day of the week. Because there are 7 days per week, we would need a distinct day to be the 22nd day. This not possible, implying that there must be one day that repeats 4 times. □

Example 4.4

$\sqrt{2}$ is irrational.

Proof. We will proceed with a proof by contradiction. Suppose that $\sqrt{2}$ is rational. Then, we can write $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}$ $b \neq 0$, and a and b share no common factors other than -1 and 1. The rest of this proof is in the lecture notes on ELMS, and is encouraged as an exercise. □

Now, we will go over **proofs of equivalence**, which is when we are required to prove a biconditional statement $p \leftrightarrow q$. In this case, we must prove p assuming q $(q \to p)$ and q assuming p $(p \to q)$.

Example 4.5

Prove that if n is an integer, then n is odd if and only if n^2 is odd. Furthermore, prove that the following statements with the integer n are also valid:

- n is even
- $n - 1$ is odd
- n^2 is even

Proof. This is left as an exercise. □

§5 Tuesday, September 27, 2022

§5.1 Exhaustive proofs

We can prove a statement by **exhaustion** by checking all possible cases that may occur in the statement and proving that the statement is either true or false.

Example 5.1
For all positive integers n with $n \leq 4$, $(n+1)^3 \geq 3$.

Example 5.2
There are no integers solutions to the equation $x^2 + 3y^2 = 8$.

§5.2 Proof by cases

We can prove a statement with **cases** by splitting the statement into multiple cases proving (or disproving) each individual case. Note that every case combined must encompass the entire statement. The following examples are left as an exercise:

Example 5.3
For every integer n, $n^2 \geq n$.

Example 5.4
If n is odd, then $n^2 = 8m + 1$for some integer m.

§5.2.1 Constructive proofs of existence

Constructive proofs of existence demonstrate the existence of a mathematical object by creating or providing a method for creating the object (from Wikipedia).

Example 5.5
$\exists a, b \in \mathbb{N}$ such that $a^b = b^a \wedge b \neq a$.

Proof. Suppose we have $a = 2$ and $b = 4$. $2^4 = 4^2$, and $2 \neq 4$. □

Example 5.6
$\exists a, b, c \in \mathbb{N}$ (all distinct) such that $a^2 + b^2 = c^2$.

Proof. Suppose we have $a = 3$, $b = 4$, and $c = 5$. Then, we have $3^2 + 4^2 = 5^2$. □

Example 5.7
23 can be written as the sum of 9 cubes of nonnegative integers.

Proof. Note that $23 = 2^3 + 2^3 + 7(1^3)$. □

Example 5.8

There is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Proof. Note that $1729 = 10^3 + 9^3 = 12^3 + 1^3$. □

§6 Thursday, September 29, 2022

Today, we will review for the midterm exam. There are lecture slides posted on ELMS.

§7 Tuesday, October 4, 2022

Midterm #1 is today.

§8 Thursday, October 6, 2022

§8.1 Universal Generalization Method of Proof

Today, we'll go over examples of proving a statement with universal generalization.

Example 8.1

$\forall n \in \mathbb{N}^{\text{even}}$, n^2 is even.

Proof. □

Example 8.2

$\forall n \in \mathbb{N}^{>0}$, $n^2 + 3n + 2$ is composite.

Proof. □

Example 8.3

$\forall n \in \mathbb{Z}^{\text{even}}$, $(-1)^n = 1$.

Proof. □

§8.2 Divisibility

Theorem 8.4

$\forall x, y, z$, $x|y$ and $y|z$ implies $x|z$.

Proof. Fill this in ASAP. □

Theorem 8.5

For any $n > 1$ and $n \in \mathbb{Z}$, we have that n is divisible by a prime number.

Proof. We will proceed by divisibility and universal generalization. Pick an arbitrary value $a \in \mathbb{Z}$ with $a > 1$. We can write a as $p_0 q_0$. If a is already a prime number, then we are done, because $a = a \cdot 1$.

If a is a composite number, then we have that both p_0 and q_0 are some factors of a, e.g. $p_0|a$ and $q_0|a$. WLOG suppose p_0 is prime. Then, we are done. If p_0 is not prime, then p_0 must be equal to $p_1 q_1$, for some factors p_1 and q_1. If p_1 and/or q_1 is a prime number, then we are done. If neither of them are prime, we can write $p_1 = p_2 q_2$. If either of these is prime, we are done. If neither of them are prime, we can iteratively repeat this process until we find a prime number. Eventually, this process will stop, and we will find a prime number that divides n. □

§8.3 Fundamental Theorem of Arithmetic

Theorem 8.6 (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and $p_1 < p_2 < \ldots < p_k$.

Example 8.7

Prove $\forall a \in \mathbb{N}^+$, $\forall q \in \mathbb{N}^{\text{prime}}$, $q|a^2 \to q|a$.

Proof. Fill this in ASAP. □

Example 8.8

Prove $\sqrt{3} \neq \mathbb{Q}$.

Proof. Fill this in ASAP. □

§9 Tuesday, October 11, 2022

§9.1 Modular Arithmetic

Definition 9.1. $a \mod n$ represents the remainder when an integer a is divided by the positive integer n. a is **congruent** to b modulo n if n divides $a - b$. a congruent to b is represented as $a \equiv b \pmod{n}$, or $a \equiv_n b$. We can also write $a \mod n \equiv b \mod n$.

Example 9.2

Is 17 congruent to 5 modulo 6? Is 24 congruent to 14 modulo 6?

Solution. Yes; No. $6|(17-5)$, but $6 \nmid (24-14)$. □

Theorem 9.3

The integers a and b are congruent modulo n if and only if there is an integer k such that $a = b + kn$.

Proof. Forward direction: $a = b + kn \to a - b = kn \to (a-b)|n \to a \equiv b \pmod{n}$, by the definition of the modulo operator. To prove the backwards direction, $a \equiv b \pmod{n} \to n|(a-b) \to nk = a - b \to a + b + kn$, once again, by the definition of the modulo operator. □

Theorem 9.4

If $a \equiv b \mod n$ and $c \equiv d \mod n$,

$$\begin{aligned} a + c &\equiv b + d \pmod{n} \\ a - c &\equiv b - d \pmod{n} \\ ac &\equiv bd \pmod{n} \\ a^m &\equiv b^m \pmod{n} \end{aligned}$$

Theorem 9.5

$\forall a, b \in \mathbb{N}$, the following are equivalent:

$$\begin{gathered} a \equiv b \pmod{n} \\ a \equiv_n b \\ n|(a-b) \\ (\exists k \in \mathbb{Z}),\ a = b + kn \end{gathered}$$

Theorem 9.6 (Quotient Remainder Theorem)

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d$$

Example 9.7

Try $n = 54$ and $d = 4$, $n = -54$ and $d = 4$, and $n = 54$ and $d = 70$ (this last case doesn't work).

Example 9.8

Prove $\forall$, $2n^2 + 3n + 2$ is not divisible by 5.

Example 9.9

$\forall n \in \mathbb{Z}$, $3 \nmid n \to n^2 \equiv_3 1$.

§9.2 Floor and Ceiling

Definition 9.10. The **floor function** is defined by $\forall x \in \mathbb{R}$ and $n \in \mathbb{Z}$, $\lfloor x \rfloor = n \leftrightarrow n \leq n < n + 1$.

Definition 9.11. The **ceiling function** is defined by $\forall x \in \mathbb{R}, n \in \mathbb{Z}$, $\lceil x \rceil = n \leftrightarrow n - 1 < x \leq n$.

Theorem 9.12

$\forall x \in \mathbb{R}$, $\forall y \in \mathbb{Z}$, $\lfloor x + y \rfloor = \lfloor x \rfloor + y$.

Theorem 9.13

The floor of $\frac{n}{2}$ is either

- $\frac{n}{2}$ when n is even, or
- $\frac{n-1}{2}$ when n is even

Note: the quiz on next Wednesday will be on modular arithmetic, as well as the floor and ceiling functions.

§10 Thursday, October 13, 2022

§10.1 Sequences, Summations, and Products

Note 10.1. I'll be taking most of my notes in this section from CLRS, as it seems more rigorous and worth reading.

Example 10.2

Find a formula for the following series: $1 + -\frac{1}{4} + \frac{1}{9} + -\frac{1}{16} + \dots$

Solution. Using summation notation, we have $\sum_{i=1}^{\infty}(-1)^{n+1}\frac{1}{i^2}$. Of course, as we haven't discussed summation notation yet, this is cheating. □

Definition 10.3. Given a sequence $a_1, a_2, \dots, a_n$ of numbers, where n is a nonnegative integer, we can write the finite sum $a_1 + a_2 + \dots + a_n$ as

$$\sum_{k=1}^{n} a_k$$

If $n = 0$, the value of the summation is defined to be 0. If we have an infinite sequence $a_1, a_2, \dots$, we can write $a_1 + a_2 + \dots$ as $\sum_{k=1}^{\infty}$, which we interpret to mean $\lim_{n\to\infty}\sum_{k=1}^{n} a_k$.

Definition 10.4. If the above limit does not exist, we say the series **diverges**. Otherwise, it **converges**. Note that we cannot always add the terms of a convergent series in any order. We can, however, rearrange the terms of an **absolutely convergent** series; that is, a series $\sum_{k=1}^{\infty} a_k$ for which the series $\sum_{k=1}^{\infty}$ also converges.

Note that summations are also linear. We can extend this property to manipulate summations using asymptotic notation, e.g.

$$\sum_{k=1}^{n}\Theta(f(k)) = \Theta\left(\sum_{k=1}^{n} f(k)\right).$$

§11 Tuesday, October 18, 2022

Today, we'll discuss **proof by induction**.

§11.1 Proof by Induction

To prove a statement is true (or false) with proof by induction, we must show that it holds (or doesn't hold) for a **base case** (usually 0 or 1), assume that it holds for an arbitrary n (the **inductive hypothesis**), and attempt to prove that it holds for $n + 1$. In this class, we will assume that it holds for an arbitrary $n - 1$, and attempt to prove a statement for n (the **inductive step**).

Example 11.1

Prove that $\forall n \in \mathbb{N}^{n\geq 1}$, $n^3 \equiv_3 n$.

Proof. Our base case is $n = 1$. $n^3 = 1$, which like 1, has a remainder of 1 when divided by 3. For our inductive hypothesis, suppose the congruence holds for n, e.g. $(n-1)^3 \equiv_3 n-1$. We will attempt to prove $n^3 \equiv_3 n$. This means $3|(n-1)^3-(n-1)^3$. Note that $(n-1)^3-(n-1) = (n-1)[(n-1)^2-1] = (n-1)(n)(n-2) = (n-2)(n-1)(n)$. Note that $n^3 - n = n(n^2-1) = n(n-1)(n+1) = n(n-1)[(n-2)+3]$, by algebra. This can be expanded as $n(n-1)(n-2)+3(n)(n-1)$. As we have $n(n-1)(n-2)$ is divisible by 3, by out inductive step, and 3 is a factor of $3n(n-1)$, we have that the sum $n(n-1)(n-2)+3n(n-1)$ also divides 3.

□

Example 11.2

Prove $\forall n \geq 1, \sum_{i=1}^{n}(4i-2) = 2n^2$.

Proof. Our base case is $n = 1$. Note that $\sum_{i=1}^{1} 4i - 2 = 4(1) - 2 = 2 = 2(1)^2$, which is true. Assume $\sum_{i=1}^{n-1}(4i-2) = 2i^2$. We will attempt to prove $\sum_{i=1}^{n}(4i-2) = 2n^2$. Note that $\sum_{i=1}^{n}(4i-2) = 2n^2 = \sum_{i=1}^{n-1}(4i-2) + (4n-2) = 2(n-1)^2 + 4n - 2$. This is equivalent to $2(n^2-2n+1)+4n-2 = 2n^2-4n+2+4n-2 = 2n$, completing the proof. □

Example 11.3

Prove $\forall n \geq 1, \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Proof. Our base case is $n = 1$. Note that $\sum_{i=1}^{1} i = 1$ and $\frac{1(2)}{2} = 1$, which means our base case holds. Assume $\sum_{i=1}^{n-1} i = \frac{(n-1)n}{2}$. We will attempt to prove $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Note that $\sum_{i=1}^{n} = \sum_{i=1}^{n-1} + n = \frac{(n-1)n}{2} + n = \frac{n^2-n+2n}{2} = \frac{n^2+n}{2} = \frac{n(n+1)}{2}$, completing the proof. □

Example 11.4

Prove $\forall n \geq 0, \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

Our base case is $n = 1$. Note that $\sum_{i=0}^{1} 2^i = 2^0 + 2^1 = 1 + 2 = 3$, and $2^{1+1} - 1 = 4 - 1 = 3$, which means our base case holds. Assume $\sum_{i=0}^{n-1} 2^i = 2^n - 1$. We will attempt to prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$. Note that $\sum_{i=0}^{n} 2^i = \sum_{i=0}^{n-1} + 2^n = 2^n - 1 + 2^n = 2(2^n) - 1 = 2^{n+1} - 1$, completing the proof.

Example 11.5

Prove $\forall n \in \mathbb{R}^{>1}, \forall n \in \mathbb{Z}^{\geq 0}, \sum_{k=0}^{k} r^k = \frac{r^{n+1}-1}{r-1}$.

Proof. Our base case is $n = 1$. Note that $\sum_{k=0}^{1} r^k = r^0 + r = r + 1$, and $\frac{r^{1+1}-1}{r-1} = \frac{(r+1)(r-1)}{r-1} = r + 1$. Note that we can cancel $r - 1$ from both sides, as $r - 1 > 0$, since $r > 1$. Thus, our base case holds. Assume $\sum_{k=0}^{n-1} r^k = \frac{r^n-1}{r-1}$. We will attempt to prove

$\sum_{k=0}^{n} r^k = \frac{r^{n+1}-1}{r-1}$. Note that $\sum_{k=0}^{n} r^k = \sum_{k=0}^{n-1} r^k + r^n = \frac{r^n-1}{r-1} + r^n = \frac{(r^n-1)+r^n(r-1)}{r-1} = \frac{(r^n-1)+r^{n+1}-r^n}{r-1} = \frac{r^{n+1}-1}{r-1}$, completing the proof. □

Example 11.6

Prove $\forall n \in \mathbb{Z}^{\geq 3}, 2n+1 < 2^n$.

Proof. Our base case is $n = 3$. Note that $2(3)+1 = 7$ and $2^3 = 8$, which means our base case holds. Assume $2(n-1)+1 < 2^{n-1}$. We will attempt to prove $2n+1 < 2^n$. Note that $2(n-1)+1 < 2^{n-1} \to 2n-1 < 2^{n-1} \to 2n < 2^{n-1}+1$. Adding 1 to both sides, we obtain $2n+1 < 2^{n-1}+2 \to 2n+1 < 2(2^{n-1}) \to 2n+1 < 2^n$, completing the proof. □

§12 Thursday, October 20, 2022

Today, we'll cover **strong induction**. Before we start, however, let's go over some more examples of proof by induction.

Example 12.1

$\forall n \in \mathbb{Z}^{\geq 2}, \forall x \in \mathbb{R}^+, 1+nx \leq (1+x)^n$.

Proof. Our base case is $n = 2$. $(1+x)^2 = x^2+2x+1$, which is greater than or equal to than $1+2x$, as $x^2 \geq 0$ for all x. Assume $1+nx \leq (1+x)^n$. We will attempt to prove $1+(n+1)x \leq (1+x)^{n+1}$. Note that $(1+x)^{n+1}$ can be rewritten as $(1+x)^n(1+x)$.

$$\begin{aligned}(1+x)^n(1+x) &\geq (1+nx)(1+x)\\ &\geq 1+x+nx+x^2\\ &\geq 1+(n+1)x+x^2\end{aligned}$$

As $(1+x)^{n+1} \geq 1+(n+1)x+x^2$, we have $(1+x)^{n+1} \geq 1+(n+1)x$, as $x^2 > 0$ (since $x \in \mathbb{R}^+$). □

Example 12.2 (Recurrence relation)

Let a_n be a sequence defined by $a_1 = 1$ and $\forall n \geq 2$, $a_n = a_{n-1} + (2n-1)$. Prove $\forall n \geq 1$, $a_n = n^2$.

Proof. Our base case is $n = 1$. $a_1 = 1 = 1^2$, which is true. Assume $a_n = n^2$. We will attempt to prove $a_{n+1} = (n+1)^2$. Note that $a_{n+1} = a_n + (2(n+1)-1) = n^2 + 2(n+1) - 1 = n^2+2n+2-1 = (n+1)^2$. □

Remark 12.3. Proofs involving recurrence relations will show up commonly in algorithms classes, especially CMSC351.

Example 12.4

Let a_n be a sequence of numbers defined by $a_0 = 1$ and $\forall n \geq 1$, $a_n = \left[\sum_{i=0}^{n-1} a_i\right] + 1$. Prove $\forall n \geq 0$, $a_n = 2^n$.

Proof. Our base case is $n = 0$. $a_0 = 1 = 2^0$, which is true. Assume $a_n = 2^n$. We will attempt to prove $a_{n+1} = 2^{n+1}$. Note that $a_{n+1} = \left[\sum_{i=0}^{n} a_i\right] + 1 = \left[\sum_{i=0}^{n-1} a_i\right] + 1 + a_n = 2^n + a_n = 2(2^n) = 2^{n+1}$. □

Example 12.5

Let a_n be a sequence defined by $a_0 = 1$, $a_1 = 1$, $a_2 = 3$, and $\forall k \in \mathbb{Z}^{\geq 3}$, $a_k = a_{k-1} + a_{k-2} - a_{k-3}$. Prove $\forall n \in \mathbb{Z}^{\geq 0}$, $a_n \in \mathbb{Z}^{\text{odd}}$.

Proof. Our base cases are $n = 0$, $n = 1$, and $n = 2$. As a_i is odd for $1 \leq n$, our base cases are satisfied. Assume $a_n \in \mathbb{Z}^{\text{odd}}$. We will attempt to prove $a_{n+1} \in \mathbb{Z}^{\text{odd}}$. Note that $a_{n+1} = a_n + a_{n-1} - a_{n-2}$. Mathematical induction does NOT work for this proof, as we do not use the inductive hypothesis in places other than the parity of a_n. As we do not know anything about the parities of a_{n-1} and a_{n-2}, induction on n is not strong enough. This motivates strong induction.

□

§12.1 Strong Induction

In **strong induction**, we assume all of the dominoes before domino n fall and then show domino n must also fall. This is frequently easier than weak induction, as our inductive hypothesis is stronger (since we are assuming more things). The structure of strong induction is as follows:

- **Claim**: $\forall n \in \mathbb{N}$, $P(n)$
- **Base Case**: Show $P(0), P(1), P(2), \ldots$ directly. The number of base cases will depend on the context of the problem, but note that it can also be 1.
- **Inductive Hypothesis**: For some $n \geq n - 1$, assume $P(i)$ holds for all $i \leq n - 1$.
- **Inductive Step**: Prove $P(n)$ must also be true, based on your assumption that P holds for all previous values

Example 12.6

Prove Example 12.5 using strong induction.

Proof. Our base cases are a_0, a_1, and a_2. As $a_0 = 1$, $a_1 = 1$, and $a_2 = 3$, and each of these is odd, our base cases are satisfied. Now, suppose each of a_n, a_{n-1}, $a_{n-2}, \ldots$ is odd. We would like to prove $a_{n+1} = a_n + a_{n-1} + a_{n-2}$ is odd. By the inductive hypothesis, as each of a_n, a_{n-1}, and a_{n-2} is odd, we have that the sum is odd. To prove this rigorously, let $a_n = 2k_1 + 1$, $a_{n-1} = 2k_2 + 1$, and $a_{n-2} = 2k_3 + 1$. $a_n + a_{n-1} + a_{n-2} = 2(k_1 + k_2 + k_3 + 1) + 1$, which is odd, as $k_1 + k_2 + k_3 \in \mathbb{Z}$ (as $\mathbb{Z}$ is closed under addition). □

Example 12.7

Let a_n be a sequence defined by $a_0 = 1$, $a_1 = 2$, and $\forall k \in \mathbb{Z}^{\geq 2}$, $a_k = a_{k-1} + a_{k-2}$. Prove $\forall n \in \mathbb{Z}^{\geq 0}, a_n \leq 2^n$.

Proof. Our base cases are $n = 0$ and 1. $a_0 = 1 = 2^0 \leq 2^0$ and $a_1 = 2^1 \leq 2^1$, meaning our base cases are satisfied. Assume for $k < n$, $a_k \leq 2^k$. We will attempt to prove $a_n \leq 2^n$. Note that $a_n = a_{n-1} + a_{n-2} \leq 2^{n-1} + 2^{n-2} \leq 2^{n-1} + 2^{n-1} = 2(2^{n-1}) = 2^n$. □

Example 12.8

Let a_n be a sequence defined by $a_0 = 0$, $a_1 = 7$, and $\forall i \geq 2$, $a_i = 2a_{i-1} + 3a_{i-2}$. Prove $\forall n \in N$, $a_n \equiv 0 \pmod 7$.

Proof. Our base cases are $n = 0$ and 1. As $a_0 = 0 \equiv 0 \pmod 7$ and $a_1 = 7 \equiv 0 \pmod 7$, our base cases are satisfied. Assume for $k < n$, $a_k \equiv 0 \pmod 7$. We will attempt to prove that $a_n \equiv 0 \pmod 7$. Note that $a_n = 2a_{n-1} + 3a_{n-2}$. By properties of modular arithmetic, we have $a_n \equiv 2a_{n-1} + 3a_{n-2} \pmod 7$, which means $a_n \equiv 2(0) + 3(0) = 0 \pmod 7$, completing the proof. □

§13 Tuesday, October 25, 2022

Let's cover some more examples of strong induction.

Example 13.1

Let a_n be a sequence defined by $a_0 = 1$ and for $n \geq 1$, $a_n = \left[\sum_{i=0}^{n-1} a_i\right] + 1$. Prove $\forall n \geq 0$, $a_n = 2^n$.

Proof. Our base case is $n = 0$. We have $a_0 = 2^0 = 1$, meaning our base case is satisfied. Assume for all $i \leq n - 1$, $a_i = 2^i$. We will attempt to prove $a_n = 2^n$. Note that $a_n = \left[\sum_{i=0}^{n-1}\right] + 1 = (a_0 + a_1 + \cdots a_{n-1}) + 1 = (2^0 + 2^1 + \cdots 2^{n-1}) + 1 = \frac{1(1-2^n)}{1-2} + 1 = -(1 - 2^n) + 1 = 2^n - 1 + 1 = 2^n$, completing the proof. Note that we used the inductive hypothesis when replacing each a_i in the summation with 2^i. □

Example 13.2

Let a_n be a sequence defined by $a_0 = 0$, $a_1 = 4$, and $\forall i \geq 2$, $a_i = 6a_{i-1} - 5a_{i-2}$. Prove $\forall n \in \mathbb{N}, a_n = 5^n - 1$.

Proof. Our base cases are a_0 and a_1. We have $a_0 = 0 = 5^0 - 1 = 1 - 1$ and $a_1 = 5^1 - 1 = 4$, meaning our base cases are satisfied. Assume $\forall i \leq n - 1$, $a_n = 5^n - 1$. We will attempt to prove $a_n = 5^n - 1$. Note that $a_n = 6a_{n-1} - 5a_{n-2} = 6 \cdot (5^{n-1} - 1) - 5 \cdot (5^{n-2} - 1) = 6 \cdot 5^{n-1} - 6 - 5^{n-1} + 5 = 5 \cdot 5^{n-1} - 6 + 5 = 5^n - 1$, completing the proof. □

Example 13.3

Prove $\forall n \geq 2$, n can be expressed as the product of primes. Note that we consider a single prime factor to be a product of primes.

Proof. Our base case is $n = 2$. As $2 = 2 \cdot 1$, our base case is satisfied (as 2 itself is prime). Assume $\forall i \leq n - 1$, i can be expressed as the product of prime numbers (where $2 \leq i \leq n - 1$. We will attempt to prove n is a product of prime numbers. We have two cases: if n is prime, then we are done. If n is composite, then, we have $n = a \cdot b$, where $2 \leq a \leq n - 1$ and $2 \leq b \leq n - 1$. By the inductive hypothesis, we have $a = p_1 p_2 \cdots p_i$ and $b = q_1 q_2 \cdots q_j$, where every p_i and q_i is a prime. Thus, $n = (p_1 p_2 \cdots p_i)(q_1 q_2 \cdots q_j)$ As each p_i and q_i is prime, we have that n can be written as a product of prime numbers, and are done. □

Remark 13.4. The above example is "half" of the Unique Prime Factorization Theorem. The other half of this theorem would entail showing that this prime factorization is *unique*.

Example 13.5 (Chocolate Bar Problem)

Suppose you have a chocolate bar that is sectioned off into n squares, arranged in a rectangle. You can break the bar into pieces along the lines separating the squares (each break must go all the way across the current piece). Prove it will always take $n - 1$ breaks to separate the bar into individual squares, no matter how you proceed.

Proof. We will proceed with strong induction on n. Our base case is $n = 1$. When the chocolate bar is only composed of 1 square, no breaks ($1 - 1 = 0$) need to be made to separate the bar into individual squares, meaning our base case is satisfied. Suppose for every chocolate bar of size $i \leq n - 1$, it takes $i - 1$ breaks to separate the bars into individual squares. We will attempt to prove that it will take $n - 1$ breaks to separate a bar of size n into individual squares. First, break the bars with n squares into two parts of size p and q. By our inductive hypothesis, it takes $p - 1$ breaks to separate a bar of size p and $q - 1$ breaks to separate a bar of size q. Hence, it takes $p - 1 + q - 1 = p + q - 2 + 1 = p + q - 1 = n - 1$ breaks to separate a bar

of size n. A 1 is added at the end to account for the first break that was used to separate the bar into two bars of size p and q. Hence, it will take $n-1$ breaks to separate a bar of size $n-1$ into individual squares. □

Let's now cover **constructive induction**. Constructive induction is a method for solving recurrences where you "guess" the general form of a formula but do not know the specific constants. Induction is used to find the specific constants, and the base case is used to verify that the formula is correct.

§13.1 Constructive Induction

Example 13.6

Find a formula $\forall n \geq 1$, $\sum_{i=1}^{n} 4i - 2$. Prove that this formula holds for all n.

Note that $\sum_{i=1}^{n} 4i - 2 = 4\sum_{i=1}^{n} i - 2\sum_{i=1}^{n} 1 = \frac{4(n)(n+1)}{2} - 2n = 2(n)(n+1) - 2n = 2n(n+1-1) = 2n^2$. Thus, we can *expect* to obtain this formula. However, in our proof, assume that the formula is a quadratic $an^2 + bn + c$. We assume it is a quadratic because the formula inside the summation is linear. Our base case is $n = 1$. Note that $\sum_{i=1}^{1} 4i - 2 = 2$ and $a(1)^2 + b(1) + c = a + b + c = 2$, meaning this formula holds for the base case. Now, assume $\sum_{i=1}^{n-1} 4i - 2 = a(n-1)^2 + b(n-1) + c$. We will attempt to prove $\sum_{i=1}^{n} 4i - 2 = an^2 + bn + c$. Note that $\sum_{i=1}^{n} = \sum_{i=1}^{n-1} + n^2 = a(n-1)^2 + b(n-1) + c + 4n - 2 = a(n^2 - 2n + 1) + bn - b + c + 4n - 2 = an^2 - 2an + a + bn - b + c + 4n - 2 = an^2 + (-2a + b + 4)n + (a - b + c - 2)$. Now, assume $an^2 + (-2a+b+4)n + (a-b+c-2) = an^2 + bn + c$. We have $b = -2a + b + 4$, $c = a - b + c - 2$, and $2 = a + b + c$ (from the base case). Solving this system of equations gives us $(a, b, c) = (2, 0, 0)$, meaning $\sum_{i=1}^{n} 4i - 2 = 2n^2$. To ensure that we are done, we must verify the base case $n = 1$. As $4(2) - 2 = 2(1^2) = 2$, we are done.

§14 Thursday, October 27, 2022

Let's cover another example of constructive induction.

Example 14.1

Let a_n be a sequence defined by $a_0 = 2$, $a_1 = 7$, and $\forall k \in \mathbb{Z}^{\geq 2}$, $a_k = 12a_{k-1} + 3a_{k-2}$. Find the smallest integers A and B such that $a_n \leq A \cdot B^n$, where $n \in \mathbb{Z}^{\geq 0}$.

Proof. Our base cases are $n = 0$ and $n = 1$. For $n = 0$, we have $a_0 = 2 \leq A \cdot B^0 = A \to A \geq 2$. For $n = 1$, we have $a_1 = 7 \leq A \cdot B^1 = AB$, or $AB \geq 7$. Assume the for all $i \leq n - 1$, $a_i \leq A \cdot B^i$. We will attempt to prove $a_n \leq A \cdot B^n$. Note that $a_n = 12a_{n-1} + 3a_{n-2} \leq 12(A \cdot B^{n-1}) + 3(A \cdot B^{n-2}) = 12AB^{n-1} + 3AB^{n-2}$. We want to find constants A and B such that $12AB^{n-1} + 3AB^{n-2} \leq AB^n$. We can now solve the following inequality:

$$\begin{aligned} 12AB^{n-1} + 3AB^{n-2} &\leq AB^n \\ 12B^{n-1} + 3B^{n-2} &\leq B^n \\ 12B + 3 &\leq B^2 \\ B^2 - 12B - 3 &\geq 0 \end{aligned}$$

Solving for B, we see $B = \frac{12 \pm \sqrt{144+12}}{2}$, or $B = \frac{12-\sqrt{156}}{2}$ or $B = \frac{12+\sqrt{156}}{2}$. From our base cases, we have $AB \geq 7$ and $A \geq 2$, implying $2B \geq 7 \to B \geq \frac{3}{2}$. As $2B \geq 7$ $B > 0$, meaning $B = \frac{12+\sqrt{156}}{2}$. To verify the base case ($AB \geq 7$), we would like to $2\left(\frac{12+\sqrt{156}}{2}\right) \geq 7$. This is true; as B must be an integer, we can round up to obtain $B = 13$. Thus, our integers A and B are 2 and 13, respectively. □

§14.1 Set Theory

Definition 14.2. A **set** is an unordered collection of elements. A set can have either a finite or infinite number of elements.

Example 14.3 (Examples of sets)

The following are sets:

- $S = \{a, b, c, d\}, a \in S$ and $e \notin S$
- $A = \{1, 2, 3\}$
- $B = \{x \in \mathbb{Z} | -4 < x < 4\}$
- $C = \{x \in \mathbb{Z}^+ | -4 < x < 4\}$

Definition 14.4. The **universal set**, usually denoted by U, is the set consisting of all possible elements in some particular situation under consideration.

Definition 14.5 (Cardinality)**.** For a set S, $n(S)$ or $|S|$ are used to refer to the cardinality of S, which is the number of elements in S.

Definition 14.6. A set A is a subset of B if $\forall x \in U, x \in A \to x \in B$. We say A is **contained** in B or that B **contains** A. $A \not\subset B \leftrightarrow (\exists x \in U)$ such that $x \in A \wedge x \notin B$.

Definition 14.7. We say sets A and B are **equal** if and only if $A \subseteq B$ and $B \subseteq A$.

Definition 14.8. A is a **proper subset** of B if and only if $A \subseteq B$ and $A \neq B$.

Definition 14.9. The following are operations used with sets:

- Union: $A \cup B = x \in U$ such that $x \in A$ or $x \in B$.
- Intersection: $A \cap B = x \in U$ such that $x \in A$ and $x \in B$.

- Complement: $A^c = x \in U$ such that $x \notin A$.
- Difference: $A - B = x \in U$ such that $x \in A$ and $x \notin B$.

Remark 14.10. $A - B = A \cap B^c$.

Definition 14.11. The **empty set**, denoted by $\emptyset$, is a set that has no elements, e.g. $\emptyset = \{\}$. The empty set has several properties that I won't include here, as most of the are quite intuitive to understand.

Definition 14.12. Sets A and B are **disjoint** if and only if A and B have no elements in common, e.g. $\forall x \in U$, $x \in A \to x \notin B$ and $x \in B \to x \notin A$.

Remark 14.13. A and B are disjoint if and only if $A \cap B = \emptyset$.

Definition 14.14. The **Cartesian Product** of two sets A and B, denoted by $A \times B$, consists of all ordered pairs (a, b) such that $a \in A$ and $b \in B$.

Definition 14.15. $\mathcal{P}(A)$ denotes the **power set** of A, which is the set of all subsets of A.

§15 Tuesday, November 1, 2022

Today, there will be a guest lecture; I will not take notes.

§16 Thursday, November 3, 2022

§16.1 Midterm # Review

Today is a review day for Midterm #2.

§17 Tuesday, November 8, 2022

Midterm #2 is today.

§18 Thursday, November 10, 2022

Today, we'll continue discussing set theory.

Theorem 18.1 (Set Properties)
If A and B are sets, we have that the following properties hold:

- $A \cup B \subseteq A$
- $AA \cup B$
- $A \cap BB$
- $B \subseteq A \cup B$

The above properties are called **inclusion** properties.

We also have **transitivity** properties:

Theorem 18.2
If A and B are sets, we have that the following property holds:

$$A \subseteq B \land B \subseteq C \to A \subseteq C$$

How do we prove set equality? To prove sets A and B are equal, e.g. $A = B$, we must prove that $A \subseteq B$ and BA. To prove a set is a subset of another set, we must take a general element in the set and prove that it must be in the other set. This brings us to the following definition:

Definition 18.3. Sets A and B are equal if and only if $A \subseteq B$ and BA.

Now that we have defined set equality, we can define more properties of sets.

Theorem 18.4 (DeMorgan's Laws)
If A and B are sets, we have

- $(A \cup B)' = A' \cap B'$
- $(A \cap B)' = A' \cap B'$

Theorem 18.5 (Distributivity)
If A and B are sets, we have

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

We can also prove two sets are equal using the above set properties. Likewise, we can derive new properties of sets from the existing properties.

§19 Tuesday, November 14, 2022

Let's continue proving set properties.

Example 19.1
Prove $A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Proof. Let $x \in A$. As $A \subseteq B$, we have $x \in B$. As $x \in A$, we also have $x \in \mathcal{P}(A)$. As $x \in B$, we also have $x \in \mathcal{P}(B)$. As $x \in \mathcal{P}(A) \to x \in \mathcal{P}(B)$, we have $\mathcal{P}(A) \subseteq \mathcal{P}(A)$. □

Example 19.2
Let $n(A)$ be a function that takes in a set as input and outputs the number of elements in the set. For finite sets A, prove that $n(A) = k \to n(\mathcal{P}(A)) = 2^k$.

Proof. We will proceed with a proof by induction. Fill this in ASAP. □

Example 19.3
Fill this in ASAP.

§19.1 Partitions of a set

Definition 19.4. A collection of nonempty sets $\{A_1, A_2, \ldots, A_n\}$ is a **partition** of a set A if and only if

1. $A = A_1 \cup A_2 \cup \cdots \cup A_n$
2. $A_1, A_2, \ldots, A_n$ are mutually disjoint

Remark 19.5. Most sets are not subsets of themselves. Russell's Paradox gives an example of this.

§20 Thursday, November 17, 2022

§20.1 Combinatorics

Combinatorics is the study of **counting** and attempts to answer the question "How many?" without actually writing down every possible choice.
Rules of sum and product We can sometimes express a set of items that we can that we wish to count as a union of disjoint sets or as a Cartesian product of sets.

Definition 20.1. The **rule of sum** says that the number of ways to choose one element from one of two disjoint sets is the sum of the cardinalities of these sets. That is, if $A \cap B = \emptyset$, $|A \cup B| = |A| + |B|$.

Definition 20.2. Suppose E is an experiment conducted through k sequential steps $s_1, s_2, \ldots, s_k$, where every s_i can be conducted in n_i different ways. The **rule of product** says that the total number of ways that E can be conducted is

$$\prod_{i=1}^{k} n_i = n_1 \cdot n_2 \cdots n_k$$

Example 20.3

How many subsets are there of a set of 4 elements $\{a, b, c, d\}$?

Solution. For each element, we are able to either include or exclude the element in the subset. Thus, our answer is $2^4 = 16$. □

§20.2 Permutations

Definition 20.4. A **permutation** of a finite set S is an ordered sequence of all the elements of S, with each element appearing exactly once.

Example 20.5

If $S = \{a, b, c\}$, S has 6 permutations $abc, acb, bac, bca, cab, cba$.

There are $n!$ permutations of a set of n elements, since we can choose the first element of the sequence in n ways, the second in $n - 1$, ways, and so on.

Definition 20.6. A **k-permutation** of S is an ordered sequence of k elements of S, with no element appearing more than once in the sequence.

Remark 20.7. An ordinary permutation is an n-permutation of an n-set.

Example 20.8

The twelve 2-permutations of the set $\{a, b, c, d\}$ are $ab, ac, ad, ba, bc, bd, ca, cb, cd$

da, db, dc.

Theorem 20.9

The number of k-permutations of an n-set is

$$n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

since we have n ways to choose the first element, $n-1$ ways to choose the second element, and so on, until we have selected k elements (where the last

§20.2.1 Combinations

Definition 20.10. A **k-combination** of an n-set is simply a k-subset of S.

Example 20.11

The 4-set $\{a, b, c, d\}$ has six 2-combinations: ab, ac, ad, bc, bd, cd.

We can construct a k-combination of an n-set by choosing k distinct elements from the n-set. The order in which we select the elements does not matter. We can express the number of k-combinations of an n-set in terms of the number of k-permutations of an n-set. Every k-set has exactly $k!$ permutations of its elements, each of which is a distinct k-permutation of the n-set. Thus, the number of k-combinations of an n-set is the number of k-permutations divided by $k!$:

$$\frac{n!}{k!(n-k)!}$$

Remark 20.12. For $k = 0$ in the above formula, we are told that there is 1 way to choose 0 elements from an n-set, not 0 (since $0! = 1$). l

§21 Tuesday, November 22, 2022

Today, we'll discuss **discrete probability**.

§21.1 Discrete Probability

As we have covered this extensively in STAT 410, I will not take notes on this section.

§22 Tuesday, November 29, 2022

We will now start discussing **functions**. We'll start with some important definitions.

Definition 22.1. A **function** assigns members of one set (the **domain**) to members of another set (the **co-domain**). If A and B are the domain and co-domain of a function f, we write $f : A \to B$.

Definition 22.2. The **range** of a function is a subset of the domain that the function "hits" when it outputs.

Definition 22.3. A function is **onto** or **surjective** if the range is equal to the entire co-domain, e.g. every element of the co-domain gets mapped to by one or more elements in the domain.

Definition 22.4. A function is **injective** if every element in the domain maps to a distinct element in the co-domain. An injective function is also called one-to-one.

Definition 22.5. A function is **bijective** if it is surjective and injective. Such a function is sometimes called a one-to-one correspondence.

Definition 22.6. Let y be an element in the co-domain of a function. The **inverse image** of y is the subset of the domain that maps to y.

Definition 22.7. Let f be a function. The **inverse** of f, denoted f^{-1}, is a function that "reverses" f.

Example 22.8

Fill this in ASAP.

§23 Thursday, December 1, 2022

§23.1 The Pigeonhole Principle

Now, we'll discuss the Pigeonhole Principle. As I have already done numerous problems using this concept in math competitions, I will refrain from writing the examples.

Theorem 23.1

Let $m, n \in \mathbb{N}^{\geq 1}$. If n pigeons fly into m pigeonholes and $n > m$, then *at least one* pigeonhole will contain more than one pigeon.

Proof. This is left as an exercise; try it on your own. □

We can also generalize the result of the Pigeonhole Principle:

Theorem 23.2

Let n and m be positive integers. Then, if there exists a positive integer k such that $n > km$ and n pigeons fly into m pigeonholes, there will be *at least one* pigeonhole with *at least* $k + 1$ pigeons.

§23.2 Cardinality and Infinity

In this lecture, we want to answer the following questions:

- Can one infinite set be "larger" than another?
- How can we compare the sizes of infinite sets?

First, let's introduce a theorem that will help us compare cardinalities:

Theorem 23.3

If A and B are sets, the following hold:

- If we can find a one-to-one function mapping A to B, then $|A| \leq |B|$
- If we can find an onto function mapping A to B, then $|A| \geq |B|$
- If we can find a bijective function mapping A to B, then $|A| = |B|$

The above ideas allow us to compare sizes of sets without explicitly counting the elements in the set; thus we can apply them to infinite sets. Before we start using them though, let's go over another few important ideas:

Theorem 23.4

If A and B are infinite sets of the same "size," then $|A \cup B| = |A|$

Similarly infinitely many identically sized infinite collections (numbered 0, 1, 2, ...) can be merged to form a collection that is no bigger than any one of those we started with. This is stated formally in the below theorem:

Theorem 23.5

Let A_0 be an infinite set, and let $A_1, A_2, \ldots A_3$ be an infinite list of sets, all the same size as A_0. Then,

$$|A_0 \cup A_1 \cup A_2 \cup \cdots \cup | = |A_0|$$

§23.3 Countability

Fact 23.6. There is no infinite set that is smaller than $\mathbb{N}$.

Definition 23.7. An infinite set that has the same cardinality as $\mathbb{N}$ is said to be **countable**. Sets that are bigger than $\mathbb{N}$ are said to be **uncountable**.

Example 23.8

Are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and the set of all finite ASCII strings countable?

Solution. Fill this in ASAP. □

§24 Tuesday, December 5, 2022

Today, we'll continue discussing cardinality and infinity.

Theorem 24.1

The set of all real numbers between 0 and 1 is uncountable.

Proof. We will proceed with contradiction. Assume the interval 0 to 1 of real numbers is countable. Let the following be a mapping from each natural number d_i to each number $0.a_{i1}a_{i2}\dots a_{in}\cdots$. We now want to find a number that is not in the above mapping, but is in the set of all real numbers in $[0, 1]$. After "creating" a mapping between each natural number and the numbers between, we can create a new number $0.k_{n+11}k_{n+12}\dots k_{n+1n+1}$ that *must* be different from every number already in the list. Hence, our the mapping $d_i \to 0.a_{i1}a_{i2}\dots a_{in}\dots$. This method is called **Cantor diagonalization**. □

§24.1 Relations

Definition 24.2. A **binary relation** on R consists of a set A, called the **domain** of R, a set B called the **co-domain** of R, and a subset of $A \times B$ called the **graph** of R.

Remark 24.3. A function $f : A \to B$ is a special case of a binary relation in which an element $a \in A$ is related to an element $b \in B$ precisely when $b = f(a)$. All relations are NOT functions, but all functions are relations. This is because there is no condition for a relation that requires every element in the domain to map to only one element in the co-domain.

As with functions, we write $R : A \to B$ to indicate that R is a relation from A to B. When the domain and codomain are the same set A we simply say the relation is "on A." Notation-wise, it's common to use aRB to mean that the pair (a, b) is in the graph of R.

Remark 24.4. Writing the relation or operator symbol between its arguments is called **infix** notation; relations use infix notation. On the other hand, mathematical operators use **prefix** notation, such as in $< (m, n)$ or $-(m, n)$.