CMSC250 Style Guide

CMSC250 Staff

March 23, 2023

Contents

1 Week 1

1.1 Style for Statements

- Variables are denoted with lowercase letters (for example p, r, s, q, etc)
- Capital letters denote a domain (for example $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{P}$)
- Logical Symbols:
  - **Negation**: $\sim, \neg, \bar{p}$
  - **Conjunction**: $\wedge$
  - **Disjunction**: $\vee$
  - **Equivalence**: $\equiv, \not\equiv$
  - **Implication**: $\Rightarrow$
  - **Biconditional**: $\Leftrightarrow$
  - **True (Tautology)**: 1
  - **False (Contradiction)**: 0

  Note: We will not be using the logical operators XOR ($\oplus$) or XNOR ($\odot$)
- Logical Precedence:
  - We prefer you to just be explicit with parenthesis to remove ambiguity, but here is the order of operations for logical symbols:
    - Parenthesis
    - NOT
    - AND
    - OR
    - Implication/Biimplication
- Other Symbols
  - Limits: $\{a_n\} \to a$
    - The sequence $\{a_n\}$ converges to the value a
  - Functions: $f(x) : \mathbb{Z} \mapsto \mathbb{R}$
    - The function $f(x)$ maps from the Integers (the domain) to the Real numbers (codomain)
- Truth Tables
  - When given two variables, the rows should go as follows: 00, 01, 10, 11. Extrapolate this for n variables.
  - Here is an example:

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

1.2 Types of Problems to Expect

- Be able to fill in a truth table from a given statement
- When given a statement, you should be able to pick out the rows in the truth table that make it True and/or False
- Know whether a given statement is True or False (or explain why it is not necessarily true is some instances)
- When given variables, be able to contruct statements both in a logical form and in English
  - Example:
    - Define p to be "I like blue" and q to be I like food. Write " I do not like blue and I like food" in the form of a statement using the variables and logical operators.
    - Answer: $\neg p \wedge q$
- "if a then b" (ie $a \Rightarrow b$) is the same as "b, if a"
- Explaining necessary and sufficient conditions
  - Example:
    - If there is smoke, then there is fire. What is the necessary and sufficient conditions of this statement
- Be able to write the inverse, converse and contrapositive of a statement
- Proving Logical Equivalence (eg. prove $a \equiv b$) using Laws of Equivalence (LOE)
  -

$$
\begin{array}{lll}
 & \text{starting statement} & \\
\equiv & \text{derived statement} & \text{justification} \\
 & \vdots & \\
\hline
\equiv & \text{ending statement} & \text{justification}
\end{array}
$$

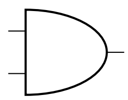
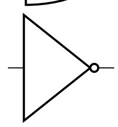
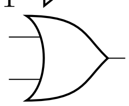
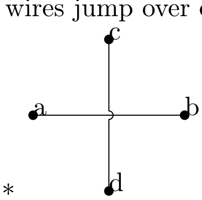
- Proving Arguments are valid (prove that $(a \wedge b) \rightarrow c$) using Rules of Inference (ROI) (can use LOE if needed):
  -

$$
\begin{array}{lll}
(1) & \text{premise one} & \\
(2) & \text{premise two} & \\
(3) & \text{argument 1} & \text{justification} \\
(4) & \text{argument 2} & \text{justification} \\
 & \vdots & \\
\hline
\therefore & conclusion & \text{justification}
\end{array}
$$

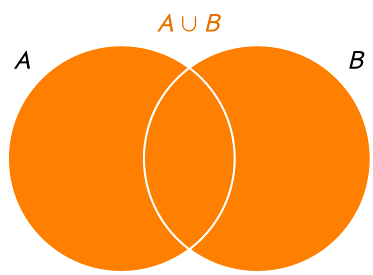
  - You may use the same LOE multiple times on one line but must recite a LOE if used later (ie. where x and y are LOEs: x, x, y can just be x, y, but x, y, x has to be that)

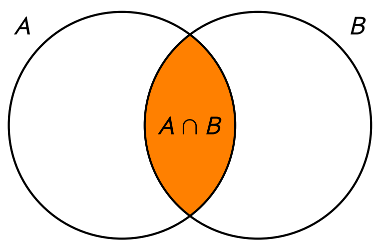
2 Week 2

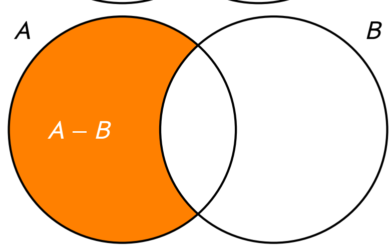
2.1 Some More Syntax

- Single Capital letters are Domains: $\mathbb{Z}, A, B$
- Uppercase Words with parenthesis are predicates. LIKES(x, y) means x likes y, $P(x)$ means x is a person, etc
- Circuits
  - We will only be using the gates:
    - AND 
    - NOT 
    - OR 
  - We will not be using other gates such as XOR, NAND, NOR, etc
  - If wires jump over each other, use the jump over symbol
    - 

  - If there is a split in a wire, put a dot to emphasize the split
- Common Domains
  - Natural Numbers (start at 0): $\mathbb{N}$
  - Integers: $\mathbb{Z}$
  - Rationals: $\mathbb{Q}$
  - Reals: $\mathbb{R}$
  - Irrationals: $\mathbb{R} \setminus \mathbb{Q}$ or $\mathbb{R} - \mathbb{Q}$
  - Primes: $\mathbb{P}$
- Sets
  - Set Symbols
    - Not in: $\notin$
    - Proper Subset: $\subset$

    - Subset: $\subseteq$
    - Equals: $=$
    - Compliment: $\overline{A}, A^c$
    - Union: $\cup$
      - $\cap_{i=1}^{\infty} A_i$ means an infinite intersection of sets A_i. Can also go to some $n \in \mathbb{N}$ instead of infinity to describe a finite intersection
    - Intersection: $\cap$
      - $\cup_{i=1}^{\infty} A_i$ means an infinite union of sets A_i. Can also go to some $n \in \mathbb{N}$ instead of infinity to describe a finite union
    - Set Minus: $\setminus$ or $-$. For example, can describe the Irrational numbers as $\mathbb{R} - \mathbb{Q}$
  - Venn Diagrams (Union, Intersection, Set Minus Visualized)
    - 

    - 

    - 

- Mathematical Symbols
  - For all: $\forall$
  - There exists: $\exists$
  - There exists a unique: $\exists!$
    - This won't come up much if at all

- The negation of $\forall$ is $\exists$ and vice versa (do not worry about $\exists!$)

- Interval Notation
  - $[x, y]$ means in the interval of x and y inclusive on both (ie $x \leq$ some value $\leq y$)
  - $(x, y]$ means in the interval of x and y inclusive on y and noninclusive on x (ie $x <$ some value $\leq y$)
  - $[x, y)$ means in the interval of x and y inclusive on x and noninclusive on y (ie $x \leq$ some value $< y$)
  - (x, y) means in the interval of x and y noninclusive on both (ie $x <$ some value $< y$)

- How to understand and create sets
  - Ellipses
    * For a small, finite set of consecutive values, we will allow the use of ellipses
    * For example: $\{1, .., 9\}$ are the integers between 1 and 9 inclusive.
  - Intervals
    * See section on interval notation for more information
    * We can thus define a set $S = [1, 4]$ to represent all the real numbers between 1 and 4 inclusive
  - Set-Builder Notation
    * This is how one should formally define a set
    * {variable name $\in D$ where D is some domain|List out conditions}
    * Examples:
      · $S = \{x \in \mathbb{Z} | (\exists k \in \mathbb{Z})[x = 2k]\}$. Thus, S is the set of even integers

    Note: When defining the conditions for a set, if a variable is needed (ie using k in the example above), one must structure it like a quantified statement as seen in the next section

      · Example that does not use another variable: $S = \{x \in \mathbb{R} | x \notin \mathbb{Q}\}$. Thus, we see S is the set of Irrational Numbers
  - Set Modification
    * We use this when making a small change to a base set. It is simply to have some simple shorthand notation, do not become reliant on these (get used to set-builder notation). Below are the ONLY ways you are allowed to do this (the base sets can be changed to be any set but generally will be our common sets)
    * $\mathbb{N}^{\neq a}$ denotes the natural numbers not equal to some value a
    * $\mathbb{R}^{\geq a}$ denotes the real numbers that are greater than or equal to some value a. Similiarly, you can use $>, \leq, <$

- $\mathbb{Z}^{\text{even}}, \mathbb{Z}^{\text{odd}}$ denotes the even and odd integers respectively

- Quantified Statements
  - What we will allow:
    - $\forall x, \exists y, x > y$ is preferred
      - In general, it should look like: quantify variable, quantify variable, ... , predicate (ie the conditions you want true for those variables) that use operators
    - $(\forall x)(\exists y)[x > y]$
    - $(\forall x(\exists y(x > y)))$
    - Will not allow $(\forall x, \exists y)[x > y]$ (ie if you are defining multiple variables, they cannot be in the same parenthesis)
  - Some Examples:
    - "For every integer, there is a real number that is smaller than it"
      - $\forall x \in \mathbb{Z}, \exists y \in \mathbb{R}, x > y$
      - $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{R})[x > y]$
      - $(\forall x \in \mathbb{Z}(\exists y \in \mathbb{R}(x > y)))$
    - "There is a prime number that is even"
      - $\exists x \in \mathbb{P}, x \equiv 0 \pmod 2$
      - $(\exists x \in \mathbb{P})[x \equiv 0 \pmod 2]$
      - $(\exists x \in \mathbb{P}(x \equiv 0 \pmod 2))$
    - "The square root of a prime number is irrational"
      - $\forall x \in \mathbb{P}, (\sqrt{x} \in \mathbb{R}) \wedge (\sqrt{x} \notin \mathbb{Q})$
      - $(\forall x \in \mathbb{P})[(\sqrt{x} \in \mathbb{R}) \wedge (\sqrt{x} \notin \mathbb{Q})]$
      - $(\forall x \in \mathbb{P}((\sqrt{x} \in \mathbb{R}) \wedge (\sqrt{x} \notin \mathbb{Q}))$
    - "The sum of two integers is also an integer"
      - $\forall x, y \in \mathbb{Z}, x + y \in \mathbb{Z}$
      - $(\forall x, y \in \mathbb{Z})[x + y \in \mathbb{Z}]$
      - $(\forall x, y \in \mathbb{Z}(x + y \in \mathbb{Z}))$

2.2 Types of Problems to Expect

- Given the the following input-output table, what is the statement and its corresponding circuit?
- what statement is is computed by the circuit? do not simplify
- show circuits influence each other
- quantify the following statements (ie. P = domain people, I(x) is the predicate that x likes ice cream, quantify the sentence, all people like ice cream)

- Going from a circuit to logical statement to a truth table (or any combination of such)
- Negating quantified statements and interpreting them
- Decide whether something is a subset, proper subset, "in" a set, and possibly interpret what a set is

3 Week 3

3.1 Number Theory

- Parity: Whether a number is even or odd
- Divides: We say a divides b (written as $a \mid b$) when $\exists k \in \mathbb{Z}, ak = b$ for $a, b \in \mathbb{Z}$
- Modulo (mod): We define $x \equiv r \pmod{m}$ as $x = km + r$, where $k \in \mathbb{Z}$ and $0 \leq r < m$. Also written as, $m \mid (x - r) \Rightarrow \exists k \in \mathbb{Z}, mk + r = x$
  - NOTE: Do not use % when talking about modulo. This is a computer science construct and does not follow the mathematical construct exactly. Stick to the form seen above
- Primes: A number p is prime if and only if the only positive divisors are 1 and p (ie $\forall x \in \mathbb{Z} \cap (1, p), x \nmid p$).
- Composite: A number c is composite if $\exists x \in \mathbb{Z} \cap (1, c), x \mid c$. That is, there is some number that divides c that is not 1 or c.

3.2 General Proof Information

- The structure listed below does not need to be *explicitly* copied, but one should understand basically every proof has this structure and includes most, if not all, the things mentioned
- Some useful terminology:
  - Axioms: Fundamental rules that are assumed to be true. These can differ problem to problem but this course does not go through using different axioms in a proof
  - Theorem: A statement (generally a well-known result) that has been proven true
  - Lemma: These are smaller proofs used within another proof to help assist in proving the main result. If you wish to use a Lemma, you must first prove it beforehand, give it a name, and then cite it using the name given in your main proof
  - QED: Written at the end of the proof to say you are done. In essence, means "Thus is is proven"
  - WLOG: Stands for "without loss of generality" and is used when there is symmetry in logic that does not need to be repeated. Helps shorten a proof
- General Proof Structure
  - **Preamble**: You should introduce information needed to start your proof here. For example:

    * the type of proof (not needed if doing direct)
    * defining any needed variables/predicated using quantification and domains
    * what you are trying to prove (this is not necessary but will be very beneficial for most proofs)
    * Assumptions
  - **Body**: Here is where you do most of the "proving". Things that usually come up:
    * Useful definitions
    * Theorems (need to be cited by name if they have one)
    * Lemmas (need to be proven first, then cited by the name you give them)
    * Axioms (need to be cited by name if they have one, but generally you don't need to use these)
    * Laws (need to be cited by name if they have one)
  - **Conclusion**: A simple sentence or two explaining what you proved and how you proved it. Also add a QED or $\blacksquare$ in the bottom right at the end of the proof

3.3 Direct Proofs

- A direct proof proceeds step-by-step from the antecedent (premises/assumptions) to the conclusion
- Follow the form $P_1 \wedge P_2 \wedge ... \wedge P_n \Rightarrow Q$, where each P_i are your predicates and Q is your conclusion (what you want to show is true)
- The general structure proof outlines a direct proof. You should start by defining variables. Then assume all P_i are true. Lastly, use definitions/algebra/theorems to deduce that Q must be true

3.4 Proof by Contrapositive

- Since this is not a direct proof, one must start the proof by saying "I will prove this using a proof by contrapositive"
- A proof by contrapositive is essentially a direct proof with one step before starting
- The key thing here is to change the statement from $P_1 \wedge P_2 \wedge ... \wedge P_n \Rightarrow Q$ to $[\neg Q \Rightarrow \neg(P_1 \wedge P_2 \wedge ... \wedge P_n)] \equiv [\neg Q \Rightarrow \neg P_1 \vee \neg P_2 \vee ... \vee \neg P_n]$, using DeMorgan's Law.
- Now, the only difference is we are assume $\neg Q$ is true and deduce that at least one of the $\neg P_i$ must be true

3.5 Proof by Contradiction

- Since this is not a direct proof, one must start the proof by saying "I will prove this using a proof by contradiction"

- A proof by contradiction consists of most of the things seen in the general proof structure

- The key difference is that we are first assuming the negation of the statement is true. We then must show that some contradiction arises (this can take many, many forms).

- Once you have found a contradiction, you must show

  - How you are able to deduce said contradiction in a logical manner

  - Why this is a contradiction to the problem (sometimes this is obvious like $1 = 0$ but it is not always this simple)

3.6 A Note About Using Cases

- Cases are used in a proof to try and break the proof down into simpler proofs

- There are two important things about cases

  - Cases MUST be exhaustive. That is, all possible cases must be covered. "All possible cases" depends on the problem so make sure you are careful about this

  - All cases must arrive at the same conclusion, namely the conclusion you are trying to prove

- Cases themselves are not a form of proof but moreso like a lemma as they are used to help solve the larger proof

- A few common cases used are (remember this is problem specific):

  - casing off whether an integer is odd or even

  - casing off whether an integer is greater than some number a and less than or equal to a

  - casing off whether an integer is equivalent to another integer under some modulo n (you would need to check equivalence of every possible integer between 0 and $n - 1$)

3.7 Correctly Styled Proof Examples

1. Prove that the product of two odd integers is odd.

   Proof:

   This can be proven directly. Let $a, b \in \mathbb{Z}^{\text{odd}}$. By the definition of an odd integer, this means that $\exists c, k \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2c+1$. We wish to show that $ab \in \mathbb{Z}^{\text{odd}}$. Hence, we must show that $\exists m \in \mathbb{Z}, ab = 2m+1$. Looking at the product ab, we see that

   $$\begin{aligned} ab &= (2k+1)(2c+1) \\ &= 4kc + 2k + 2c + 1 \\ &= 2(2kc + k + c) + 1 \end{aligned}$$

   Since the integers are closed under addition and multiplication, it must be the case that $2kc + k + c \in \mathbb{Z}$. Let $m \in \mathbb{Z}$ such that $m = 2kc + k + c$. Thus, $ab = 2m+1$. Hence, $ab \in \mathbb{Z}^{\text{odd}}$. Therefore, we have shown that the product of two odd integers is odd. ■

2. Prove that, for an integer a, if $3 \mid a^2$, then $3 \mid a$.

   Proof:

   This can be proven via a proof by contrapositive. The contrapostive is stated as such: $3 \nmid a \Rightarrow 3 \nmid a^2$, for some integer a. First, assume that $3 \nmid a$. Therefore, we know that either $a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$. I will break this into these two cases.

   Case 1: $a \equiv 1 \pmod 3$
   Assume that $a \equiv 1 \pmod 3$. Thus, $\exists k \in \mathbb{Z}, a = 3k+1$. We wish to show that $3 \nmid a^2$. We see that

   $$\begin{aligned} a^2 &= (3k+1)(3k+1) \\ &= 9k^2 + 3k + 3k + 1 \\ &= 9k^2 + 6k + 1 \\ &= 3(3k^2 + 2k) + 1 \end{aligned}$$

   Since the integers are closed under multiplication and addition, it must be the case that $3k^2+2k \in \mathbb{Z}$. Define $m = 3k^2+2k$. Thus, $a^2 = 3m+1 \Rightarrow a^2 \equiv 1 \pmod 3$. Therefore, we have shown that $3 \nmid a^2$.

   Case 2: $a \equiv 2 \pmod 3$
   Assume that $a \equiv 2 \pmod 3$. Thus, $\exists k \in \mathbb{Z}, a = 3k+2$. We wish to show

that $3 \nmid a^2$. We see that

$$\begin{aligned} a^2 &= (3k+2)(3k+2) \\ &= 9k^2 + 6k + 6k + 4 \\ &= 9k^2 + 12k + 3 + 1 \\ &= 3(3k^2 + 4k + 1) + 1 \end{aligned}$$

Since the integers are closed under multiplication and addition, it must be the case that $3k^2 + 4k + 1 \in \mathbb{Z}$. Define $m = 3k^2 + 4k + 1$. Thus, $a^2 = 3m + 2 \Rightarrow a^2 \equiv 2 \pmod 3$. Therefore, we have shown that $3 \nmid a^2$.

Therefore, we have shown in all cases that $3 \nmid a \Rightarrow 3 \nmid a^2$, for an integer a. Due to the contrapostive being logically equivalent to the original statement, we have also proven that for an integer a, if $3 \mid a^2$, then $3 \mid a$. ■

3. Prove that $\sqrt{2}$ is irrational.

Lemma 1: For an integer x, if x^2 is even, then x is even.

This can be proven via a proof by contrapostive. The contrapostive is: if x is odd, then x^2 is odd.

Assume that x is odd. Then $\exists k \in \mathbb{Z}, x = 2k + 1$. We see that

$$\begin{aligned} x^2 &= (2k+1)(2k+1) \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Since the integers are closed under multiplication and addition, we know that $2k^2+2k \in \mathbb{Z}$. Define $m \in \mathbb{Z}$ such that $m = 2k^2+2k$. Thus, $x^2 = 2m+1$. Therefore, x^2 is odd.

Since we have proven the contrapositive true, it must be the case that the original statement is true. Therefore, for an integer x, if x^2 is even, then x is even. ■

Proof:

This can be done via a proof by contradiction. First, we assume the negation is true, that is, assume that $\sqrt{2} \notin \mathbb{R} - \mathbb{Q}$. Hence, we can say that $\sqrt{2} \in \mathbb{Q}$. By definition, this means that $\exists p, q \in \mathbb{Z}, q \neq 0, \sqrt{2} = \frac{p}{q}$. We know that any fraction can be put into its simplified form, that is to say that p and q share no common factors (or $\gcd(p, q) = 1$ but we have not touched gcd in this class).

We now see that $\sqrt{2} = \frac{p}{q} \Rightarrow p = q\sqrt{2} \Rightarrow p^2 = 2q^2$. Hence, p^2 is even. By Lemma 1, we know that p is even. Thus, $\exists k \in \mathbb{Z}, p = 2k$. We see that

$2q^2 = p^2 \Rightarrow 2q^2 = (2k)^2 \Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2k^2$. Hence, we have shown that q^2 is even and by Lemma 1, q must then be even.

However, we assume that p and q shared no common factors, but we have shown that they both share a common factor of 2, a contradiction. Therefore, the original statement must be true. That is, $\sqrt{2} \in \mathbb{R} - \mathbb{Q}$. Therefore, $\sqrt{2}$ is irrational. ■

4 Week 4

4.1 Advanced Sets

- Some assumptions you can make (so long as we don't ask you to prove it or otherwise stated)
  - closure under addition, subtraction, and multiplication on $\mathbb{Z}$
  - closure under addition and multiplication on $\mathbb{N}$
  - closure under addition, multiplication, subtraction, and division on $\mathbb{R}$
  - closure under addition and multiplication on $\mathbb{N}^{>0}$
  - closure under multiplication and division on $\mathbb{Q}^{\neq 0}$
  - closure under addition, multiplication, and subtraction on $\mathbb{Q}$,
  - $(\forall x \in \mathbb{Z}\mathbb{N})[x \notin \mathbb{Z}^{\text{even}} \Rightarrow x \in \mathbb{Z}^{\text{odd}}]$
  - $(\forall x \in \mathbb{Z}\mathbb{N})[x \notin \mathbb{Z}^{\text{odd}} \Rightarrow x \in \mathbb{Z}^{\text{even}}]$
  - For any positive integer greater than 1, there is a set of unique prime factors which when multiplied together equal that integer (ie unique prime factorization for $n \in \mathbb{Z}^{>1}$)
- For a nested set, write out terms in order of cardinality of elements. For example: $\mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$
- Useful Concepts:
  - Cardinality: The number of element in a set A denoted by $|A|$
  - Powerset: The set of all possible subsets of a set A denoted by $\mathcal{P}(A)$
  - Partition: A set of pairwise disjoint non-empty sets (ie no set can be the $\varnothing$ and between any two sets, their intersection is $\varnothing$)
  - Cartesian Product: For sets A and B, we define the Cartesian product as follows: $A \times B = \{(a,b) | a \in A \wedge b \in B\}$. This can be done over any number of sets (but generally two)

4.2 Relations

- Relations are defined as a set of tuples that are related under some relation R. We are allowing a few ways to define a relation:
  - $A \times A, R : \{(x,y) | x + y \geq 100\}$
    - This can be read as "x is related to y under relation R if and only if $x + y \geq 100$".
  - $R : (\{(x,y) | x + y \geq 100\} \subseteq A \times A)$
  - $R \subseteq A \times A, R = \{(x,y) |$ Conditions for relation$\}$

- Or simply use set builder notation like so $R = \{(x, y) \in A \times A | x + y \geq 100\}$

- Some more style for relations
  - Many times, we wish to talk about a specific element of a relation. To do this you can say, for a relation $R \subseteq A \times B$:
    * aRb
    * $(a, b) \in R$
    * $a \sim_R b$ (not as common but accepted)
  - These all say that a is related to b under the relation R. Try to stay consistent when picking one of these.

- Properties of relations
  - For a relation $R \subseteq A \times A$
    * Reflective: $(\forall a \in A)[aRa]$
    * Symmetric: $(\forall x, y \in A)[(x, y) \in R \Rightarrow (y, x) \in R]$
    * Transitive: $(\forall x, y, z \in A)[(x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R]$
    * Equivalence Relation: A relation that is reflexive, symmetric, and transitive

4.3 Functions

- Functions are just a subset of relations. That is, all functions are relations with the property that, for a function $f : A \to B$,
  - $(\forall x \in A)(\exists! y \in B)[f(x) = y]$

- Style for defining functions
  - For a domain A and codomain B, we say $f : A \to B$ to mean f takes values in A and produces values in B, we then define the function as so $f(x) = x^2$.
  - In general, $f : A \to B, f(x) = x^2$. You need to always define your domain, codomain, and the function equation.
  - You can also define a piecewise function like so, $f : R \to R$

$$f(x) = \begin{cases} x & \text{if } x < 0 \\ x^2 & \text{if } x \geq 0 \end{cases} \tag{1}$$

  - Be careful with piecewise functions. You must define it so that your whole domain is obtained

- Properties of functions
  - Injective (one-to-one): $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
  - Surjective (onto): $\forall y \in B, \exists x \in A, f(x) = y$
  - Bijective (both injective and surjective)

5 Week 5

5.1 Set Proofs

- Set proofs are done the same way all other proofs are done (ie using a proof strategy and applying definitions and allowed assumptions)
- You are allowed to assume the properties given in the sets table unless stated otherwise
- Some useful definitions/properties
  - $A \subseteq B \iff \forall x \in A, x \in B$
  - $A = B \iff A \subseteq B \wedge B \subseteq A$ (also known as double containment)
  - $x \in A \cap B \iff x \in A \wedge x \in B$
  - $x \in A \cup B \iff x \in A \vee x \in B$
  - $x \in A^c \iff x \notin A$

5.2 Countability

- How can we prove a set is countable or uncountable?
  - Countable
    - Give an explicit listing of the elements in the set (with some sort of pattern like the snaking patter for $\mathbb{Q}^+$)
      - For something like proving $\mathbb{Q}^+$ is countable, it is necessary to construct the "grid", explain why this grid represents all of $\mathbb{Q}^+$, and then explain the "algorithm" used to obtain values (ie explain the snaking pattern)
    - If you can find a bijection from $\mathbb{N}$ to another set A, then A is countable
    - (Generalized Above Statement) If you can find a bijection from a countable set to another set A, then A is countable
  - Uncountable
    - If you can find a bijection from an uncountable set to another set A, then A is uncountable
    - Cantor's Diagonalization Proof
- Some assumptions you can make
  - $\mathbb{N}$ is countable
  - If B is a countable set and $A \subseteq B$, then A is countable
  - If A is an uncountable set and $A \subseteq B$, then B is uncountable

6 Week 6

6.1 Weak Induction

- There are 4 main steps (can be broken into 3) of an induction proof:
  - Step 0 (if you will): State that "I will prove this via a proof by weak induction" since we state our proof types when we are not doing a simple direct proof
  - **Base Case**: Here we wish to show the predicate is true for the first thing in our inductive set
  - **Inductive Hypothesis**: Here, we need to assume that for some arbitrary $k \geq$ our "largest base case" (ie if proving a statement for all $\mathbb{N}$, we assume $k \geq 0$) that $P(k)$ is true
    * The reason for this assumption goes back to how we prove any statement of the form $p \Rightarrow q$. We assume p and show that q must follow
    * For induction p is $P(k)$ and q is $P(k+1)$ making the proof: $P(k) \Rightarrow P(k+1)$
  - **Inductive Step**: Here, we need to deduce from our assumption of $P(k)$, that $P(k+1)$ holds
    * If you choose to not have an Inductive Hypothesis, you must still have the same assumption in your Inductive Step
    * You cannot disregard this assumption. It must be stated before trying to show $P(k+1)$
  - **Conclusion**: Here, we just need to restate what we have proven just like in our other proof strategies.
- On the next pages are a couple exams of well-styled weak induction proofs

6.2 Weak Induction Practice Problems

1. Prove that $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \in \mathbb{N}$

   Proof:
   I will prove this via a proof by weak induction. Define $P(n)$ as

   $$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

   Base Case: $n = 0$

   $$\sum_{i=0}^{0} i^2 = 0 \text{ and } \frac{0(0+1)(2(0)+1)}{6} = 0$$

   Hence $P(0)$ is true.

   Inductive Hypothesis:
   Assume for some arbitrary $k \in \mathbb{N}$ with $k \geq 0$ that $P(k)$ is true.

   Inductive Step:
   We wish to show that $P(k+1)$ is true (ie $\sum_{i=0}^{k+1} i^2 = \frac{(k+1)(2k+3)(k+2)}{6}$). Notice

   $$\begin{aligned}
   \sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^{k} i^2 + (k+1)^2 && \text{(Breaking up sum)} \\
   &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 && \text{(By the IH)} \\
   &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
   &= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} \\
   &= \frac{(k+1)[2k^2 + k + 2k + 6]}{6} \\
   &= \frac{(k+1)(2k^2 + 7k + 6)}{6} \\
   &= \frac{(k+1)(2k+3)(k+2)}{6}
   \end{aligned}$$

   Hence $P(k+1)$ is true. Therefore, we have shown that $P(k) \Rightarrow P(k+1)$.

   Conclusion: By the Principal of Mathematical Induction, we have shown that $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \in \mathbb{N}$. ■

2. Prove that $\prod_2^n (1 - \frac{1}{i^2}) = \frac{n+1}{2n}$ for all $n \in \mathbb{N}^{\geq 2}$

Proof:
I will prove this via a proof by weak induction. Define $P(n)$ as

$$\prod_2^n (1 - \frac{1}{i^2}) = \frac{n+1}{2n}$$

Base Case: $n = 2$

$$\prod_2^2 (1 - \frac{1}{i^2}) = 1 - \frac{1}{2^2} = 1 - \frac{1}{4} = \frac{3}{4} \text{ and } \frac{2+1}{2(2)} = \frac{3}{4}$$

Hence $P(2)$ is true.

Inductive Step:
Assume for some arbitrary $k \in \mathbb{N}$ with $k \geq 2$ that $P(k)$ is true. We wish to show that $P(k+1)$ is true (ie $\prod_2^{k+1} (1 - \frac{1}{i^2}) = \frac{k+2}{2k+2}$). Notice

$$\begin{aligned}
\prod_2^{k+1} (1 - \frac{1}{i^2}) &= (1 - \frac{1}{(k+1)^2}) \prod_2^k (1 - \frac{1}{i^2}) && \text{(Breaking up product)} \\
&= (1 - \frac{1}{(k+1)^2})(\frac{k+1}{2k}) && \text{(By our assumption)} \\
&= (\frac{(k+1)^2 - 1}{(k+1)^2})(\frac{k+1}{2k}) \\
&= \frac{(k+1)^2 - 1}{2k(k+1)} \\
&= \frac{k^2 + 2k + 1 - 1}{2k(k+1)} \\
&= \frac{k^2 + 2k}{2k(k+1)} \\
&= \frac{k(k+2)}{2k(k+1)} \\
&= \frac{k+2}{2(k+1)}
\end{aligned}$$

Hence $P(k + 1)$ is true. Therefore, we have shown that $P(k) \Rightarrow P(k+1)$.

Conclusion: By the Principal of Mathematical Induction, we have shown that $\prod_2^n (1 - \frac{1}{i^2}) = \frac{n+1}{2n}$ for all $n \in \mathbb{N}^{\geq 2}$. ■

6.3 Strong Induction

- Strong Induction has the same structure as weak induction with just a small change in the inductive hypothesis. Reference all the other steps in the previous section and take note of the change in the IH here:
  - Step 0 (if you will): State that "I will prove this via a proof by strong induction" since we state our proof types when we are not doing a simple direct proof
  - **Base Cases**: Here we wish to show the predicate is true for the first things in our set.
    - The amount of base cases needed is problem dependent.
    - If you only need one base case, chances are you could have used weak induction.
  - **Inductive Hypothesis**: Assume for some arbitrary $k \geq$ largest base case, $\forall i$, lowest base case $\leq i \leq k$, that $P(i)$ is true
    - This can be thought of as assuming $P(0) \wedge P(1) \wedge ... \wedge P(k)$ are all true (when using $\mathbb{N}$ as the set we are proving something for)
  - **Inductive Step**: Here, we need to deduce from our assumption of $P(k)$, that $P(k+1)$ holds
    - If you choose to not have an Inductive Hypothesis, you must still have the same assumption in your Inductive Step
    - You cannot disregard this assumption. It must be stated before trying to show $P(k+1)$
  - **Conclusion**: Here, we just need to restate what we have proven just like in our other proof strategies.
- It is nice to note that weak induction is just a special case of strong induction.
  - *Technically*, you never actually need weak induction as strong can cover any weak induction proof. However, it is important to know when strong is needed vs weak.
  - You should be using the correct form of induction for a problem which usually is apparent in the problem you are given or when you reach the inductive step you need to rely on more than just the value previous.
- An example of a correctly styled strong induction proof is given on the next page

6.4 Strong Induction Practice Problem

Define

$$a_n = \begin{cases} 0 & \text{when } n = 0 \\ 4 & \text{when } n = 1 \\ 6a_{n-1} - 5a_{n-2} & \text{when } n > 1 \end{cases} \tag{2}$$

Prove that $a_n = 5^n - 1$ for all $n \in \mathbb{N}$

Proof:
I will prove this via strong induction. Define $P(n) : a_n = 5^n - 1$.

Base Cases:
$n = 0$: $a_0 = 0$ and $5^0 - 1 = 1 - 1 = 0$. Thus, $P(0)$ is true.
$n = 1$: $a_1 = 4$ and $5^1 - 1 = 5 - 1 = 4$. Thus, $P(1)$ is true.

Inductive Hypothesis (IH):
Assume for some arbitrary $k \geq 1$ that $\forall i, 0 \leq i \leq k, P(i)$ is true.

Inductive Step: We wish to show that $P(k+1)$ is true. That is, $a_{k+1} = 5^{k+1} - 1$.
First, we start with a_{k+1},

$$\begin{aligned} a_{k+1} &= 6a_k - 5a_{k-1} \\ &= 6(5^k - 1) - 5(5^{k-1} - 1) && \text{(By the IH)} \\ &= 6(5^k) - 6 - 5(5^{k-1}) - 5 \\ &= 6(5^k) - 5^k - 6 + 5 \\ &= 5(5^k) - 1 \\ &= 5^{k+1} - 1 \end{aligned}$$

Therefore, we have shown $P(k + 1)$ is true.

Conclusion:
By the Principle of Mathematical Induction, $a_n = 5^n - 1$ for all $n \in \mathbb{N}$. ■

6.5 Structural Induction

- Structural Induction has the same structure as the induction proofs we have already seen. The difference here lies in that we are proving a statement over infinite structures that are **recursively** defined. Before, we had sets with some type of order; however, here we don't.
  - Step 0 (if you will): State that "I will prove this via a proof by structural induction" since we state our proof types when we are not doing a simple direct proof
  - **Base Case(s)**: Here we wish to show the predicate is true for the first thing(s) in our set.
    - The amount of base cases needed is problem dependent.
  - **Inductive Hypothesis**: The assumption for a structural induction proof is a bit hard to generalize. The best way to put it would be to say "assume for some arbitrary element (this depends on what the structure is) that P(element) is true. Sometimes we only need one element. Other times we made need multiple (for example proving something for binary trees means I need 2 arbitrary trees).
  - **Inductive Step**: Since we have a recursively defined structure, once we start with an arbitrary element in our IH, we should recursively create more elements. The idea is that we need to show that the predicate P holds for all the recursively generated elements
    - If you choose to not have an Inductive Hypothesis, you must still have the same assumption in your Inductive Step
    - You cannot disregard this assumption.
  - **Conclusion**: Here, we just need to restate what we have proven just like in our other proof strategies.
- It is nice to note that weak induction is just a special case of strong induction.
- An example of a correctly styled structural induction proof is given on the next page

6.6 Structural Induction Practice

1. Consider the set S where $0 \in S \wedge [x \in S \Rightarrow 2x+1 \in S]$. Prove that $S \subseteq \{2^n - 1 | n \in \mathbb{N}\}$

   Proof: I will prove this via structural induction.

   Base Case:
   $0 \in S$: $0 = 2^0 - 1$. Therefore, $0 \in \{2^n - 1 | n \in \mathbb{N}\}$.

   Inductive Hypothesis:
   Assume for an arbitrary $s \in S$ that $\exists n \in \mathbb{N}, s = 2^n - 1$. (ie that $s \in \{2^n - 1 | n \in \mathbb{N}\}$.

   Inductive Step:
   We know that since $s \in S$, by the definition of S, we recursively add the element $2s+1$. Therefore, we wish to show that $2s + 1 \in \{2^n - 1 | n \in \mathbb{N}\}$. Notice,

$$\begin{aligned} 2s + 1 &= 2(2^n - 1) + 1 && \text{(By the IH)} \\ &= 2^{n+1} - 2 + 1 \\ &= 2^{n+1} - 1 \\ &= 2^q - 1 && \text{(For some } q \in \mathbb{N} \text{ by closure of addition under } \mathbb{N}) \end{aligned}$$

   Therefore, we have that $2s + 1 \in \{2^n - 1 | n \in \mathbb{N}\}$.

   Conclusion:
   By the Principle of Mathematical Induction, we have shown that for set S where $0 \in S \wedge [x \in S \Rightarrow 2x+1 \in S]$, $S \subseteq \{2^n - 1 | n \in \mathbb{N}\}$. ■

2. Define $N(T)$ to be the number of nodes in a tree T and $E(T)$ to be the number of edges in a tree T. Define B to be the set of binary trees. Prove that $\forall T \in B, N(T) = E(T) + 1$.

   Proof:
   First, recall that for the set of binary trees B, that a singular node in is B and if T_1, T_2 are two trees in B then a node attached to T_1 is in B, a node attached to T_2 is in B, and finally a node attached to both T_1 and T_2 is in B. Now for the proof:

   I will prove this via structural induction.

   Base Case:
   A singular node: We know that N(A singular node) $= 1$ and E(A singular node) $= 0$. Hence N(A singular node) $= E$(A singular node) $+ 1$. Therefore, the

base case is proven.

Inductive Hypothesis:
Assume for two arbitrary trees $T_1, T_2 \in B$ that $N(T_1) = E(T_1) = 1$ and $N(T_2) = E(T_2) + 1$.

Inductive Step:
We wish to show that attaching a node to T_1, attaching a node to T_2, and attaching a node to both T_1 and T_2 will follow the statement.

Part 1: Attaching a node to T_1
Call this a new tree T_p. Then clearly, we have added only one node to T_1 and connected the node to T_1 with one edge. Hence,

$$\begin{aligned} N(T_p) &= N(T_1) + 1 \\ &= (E(T_1) + 1) + 1 && \text{(By the IH)} \\ &= E(T_p) + 1 \end{aligned}$$

Hence, we have show the statement is true for this part.

Part 2: Attaching a node to T_2
Call this a new tree T_q. Then clearly, we have added only one node to T_2 and connected the node to T_2 with one edge. Hence,

$$\begin{aligned} N(T_q) &= N(T_2) + 1 \\ &= (E(T_2) + 1) + 1 && \text{(By the IH)} \\ &= E(T_q) + 1 \end{aligned}$$

Hence, we have show the statement is true for this part.

Part 3: Attaching a node to T_1 and T_2
Call this a new tree T_m. Then clearly, we have added only one node to T_1 and T_2 and connected the node to T_1 with one edge and connected to T_2 with another edge. Hence,

$$\begin{aligned} N(T_m) &= N(T_1)N(T_2) + 1 \\ &= (E(T_1) + 1) + (E(T_2) + 1) + 1 && \text{(By the IH)} \\ &= (E(T_1) + E(T_2) + 2) + 1 \\ &= E(T_m) + 1 \end{aligned}$$

Hence, we have show the statement is true for this part.

Conclusion:
By the Principal of Mathematical Induction, we have shown that $\forall T \in B, N(T) = E(T) + 1$. ∎

7 Week 7

7.1 Combinatorics

- For notation of choose, we will accept:
  - $\binom{n}{k}$
  - ${}_nC_k$
  - $C(n,k)$
- For permutations:
  - ${}_nP_k$
  - $P(n,k)$
- To denote the probability of an event E simply use $P(E)$
- To denote conditional probability: $P(A|B)$, which means the probability of A given B has happened
- $\mathbb{E}[X]$ is commonly used to denote the expected value of a variable X
- For a counting/probability problem, it is helpful, but not mandatory, to state where each of your values are coming from and why you can/are add/mult/divide/subtract them

8 Useful Tables

Commutative Laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative Laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive Laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity Laws	$p \wedge 1 \equiv p$	$p \vee 0 \equiv p$
Negation Laws	$p \vee {\sim}p \equiv 1$	$p \wedge {\sim}p \equiv 0$
Double Negation Law	${\sim}({\sim}p) \equiv p$	
Idempotent Laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal Bound Laws	$p \vee 1 \equiv 1$	$p \wedge 0 \equiv 0$
DeMorgan's Laws	${\sim}(p \wedge q) \equiv {\sim}p \vee {\sim}q$	${\sim}(p \vee q) \equiv {\sim}p \wedge {\sim}q$
Absorption Laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation Laws of t and c	${\sim}1 \equiv 0$	${\sim}0 \equiv 1$
Definition of Implication	$p \Rightarrow q \equiv {\sim}p \vee q$	
Definition of Biconditional	$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \wedge q) \vee {\sim}(p \vee q)$	
Contrapositive	$p \Rightarrow q \equiv {\sim}q \Rightarrow {\sim}p$	

Table 1: Laws of Equivalence

Modus Ponens	Modus Tollens	Generalization
$p \Rightarrow q$ p $\therefore \quad q$	$p \Rightarrow q$ ${\sim}q$ $\therefore \quad {\sim}p$	p $\therefore \quad p \vee q$
Specialization	Conjunction	Elimination
$p \wedge q$ $\therefore \quad p$	p q $\therefore \quad p \wedge q$	$p \vee q$ ${\sim}p$ $\therefore \quad q$
Transitivity	Cases	Contradiction
$p \Rightarrow q$ $q \Rightarrow r$ $\therefore \quad p \Rightarrow r$	$p \vee q$ $p \Rightarrow r$ $q \Rightarrow r$ $\therefore \quad r$	${\sim}p \Rightarrow 0$ $\therefore \quad p$
Dilema		
$(p \Rightarrow q) \wedge (r \Rightarrow s)$ $(p \vee r)$ $\therefore \quad (q \vee s)$		

Table 2: Rules of Inference

Commutative	$A \cup B = B \cup A$ and $A \cap B = B \cap A$
Associative	$A \cup (B \cup C) = (A \cup B) \cup C$ and $A \cap (B \cap C) = (A \cap B) \cap C$
Distributive	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Identity	$A \cup \emptyset = A$ and $A \cap U = A$
Complement	$A \cup A^c = U$ and $A \cap A^c = \emptyset$
Double Complement	$(A^c)^c = A$
Idempotent	$A \cup A = A$ and $A \cap A = A$
Universal Bound	$A \cup U = U$ and $A \cap \emptyset = \emptyset$
DeMorgan's	$(A \cap B)^c = A^c \cup B^c$ and $(A \cup B)^c = A^c \cap B^c$
Absorption	$A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$
Complement of $\emptyset$ and U	$U^c = \emptyset$ and $\emptyset^c = U$
Set Difference	$A - B = A \cap B^c$