Discrete Math Notes

Allen Li

July 23, 2020

Contents

Chapter 1

Speaking Mathematically

1.1 Statements

1.1.1 The Three Types of Statements

1. Universal Statement: Statement that applies "for all"
   - Ex: For all real numbers x, $x^2 \geq 0$
   - Key Words: "For All"
2. Conditional Statement: If one thing is true then some other thing must be true
   - Key Words: "If, then"
3. Existential Statement: Statement that says there is at least one thing for which property is true
   - There exists an even prime number.
   - Key Words: "There exists"

   We use these three statements in order to classify different statements.

1.1.2 Universal Conditional Statements

Ex: For all real numbers, if $|x| > 1$, then $x^2 > 1$.

This statement is universal because it has the "for all", and conditional because it has "if".

1.1.3 Universal Existential Statement

Ex: For all integers n, there exists another integer m, such that $n < m$.

This statement is universal again because it has the "for all", and existential because of the "there exists".

1.1.4 Existential Universal Statement

Ex. There exists a positive integer that is less than all the positive integers.

See above reasoning.

1.2 Set Builder Notation

A set is simply defined as a collection of objects. The size of a set is the number of unique elements in the set.

1.2.1 Set Roster Notation

- Example set: $A = \{a, b, c\}$
- As shown, sets can include anything.

1.2.2 Set Builder Notation

- Example set: $A = \{x \in \mathbb{R} \mid -1 \leq x < 5\}$
- $0 \in A$, $-2 \notin A$
- Empty Set: $\{\}, \phi$
- Universal Set: u, set containing all objects, all other sets are proper subsets.
- Subsets: $A \subseteq B$ if for any element $a \in A$, $a \in B$
- By definition, $\phi \subseteq A$
- Proper subset: $A \subset B$ means all elements in A are also in B, and there exist elements in B that do not exist in A.
- $\forall$: for all, $\exists$: there exists

We actually cannot use set roster notation most of the time. It is not countable.

1.2.3 Cartesian Products

- $A \times B = \{(x, y) \mid x \in A, y \in B\}$
- Number of elements in $A \times B$ = sizes multiplied together
- This was introduced in an effort to introduce ordered pairs (differentiation of (a, b) and (b, a))
- Because of this, $A \times B \neq B \times A$

1.3 The Language of Relations and Functions

1. Relations on sets
    - Definition: a relation from set A to set B is a subset of $A \times B$. More formally, for some relation x, $x \subseteq A \times B$
    - We denote a relation between x_1 and x_2 as $x_1 \, R \, x_2$ provided that x is in $A \times B$.
    - It can be proved intuitively that a set with n elements has 2^n subsets.

- Domain and co domain of $A \times B$ is simply A and B respectively.

2. Function from A to B
   - Definition: a function is a relation such that $\forall x \in A, \exists y \in B \mid (x, y) \in F$ where $F : A \mapsto B$
   - If $(x, y) \in F$ and $(x, z) \in F$ then $(y, z) \in F$.
   - In other words, every element in A must have exactly one distinct image.
3. Extra Function Terminology
   - Squaring function: $x \mapsto x^2$
   - Successor function: $x \mapsto x + 1$
   - Constant function: $x \mapsto C$

Chapter 2

The Logic of Compound Statements

2.1 Logical Form and Logical Equivalence

An argument is a sequence of statements aimed at demonstrating the truth of an assertion.

- The assertion at the end of the sequence is called the conclusion, and the preceding statements are called premises.
- We commonly use the variables p q and r to represent component sentences.

A statement (or proposition) is a sentence that is true or false but not both. Further terminology:

- The symbol $\sim$ denotes not, $\wedge$ denotes and, and $\vee$ denotes or.
- And, or, and not can easily be represented using truth tables.
- Set up the truth table such that each group of columns builds off of the last.
- Two statement forms are logically equivalent iff they have identical truth table outputs. This is represented as $P \equiv Q$.
- Tautology $\mathbf{t}$: A statement form that is always true regardless of the truth values substituted
- Contradiction $\mathbf{c}$: opposite of tautology
- $p \wedge \mathbf{t} \equiv p$, $p \vee \mathbf{c} \equiv p$.
- Absorption laws: $p \vee (p \wedge q) \equiv p$, $p \wedge (p \vee q) \equiv p$
- See page 35 of the Discrete Math Textbook for a complete table on logical equivalences.

De Morgan's Laws: $\sim(p \wedge q) \equiv \sim p \vee \sim q$, $\sim(p \vee q) \equiv \sim p \wedge \sim q$.

Caution: De Morgan's Laws can only be used between complete statements on each side.

2.2 Conditional Statements

Logic flows from a hypothesis to a conclusion. The aim is to frame it as an "if, then". Given hypothesis p and conclusion q, we represent this as

$$p \to q.$$

The only combination of circumstances in which you would call a conditional sentence false occurs when the hypothesis is true and the conclusion is false. If the statement is true because the hypothesis is false, this is called vacuously true.

Note that in order of operations, $\to$ is performed last, and also note that

$$p \to q \equiv p \vee \sim q.$$

.

Helpful Information:

- The negation of "if p then q" is logically equivalent to "p and not q".
- $p \to q \equiv \sim q \to \sim p$.
- While the converse is not equivalent to the statement, the converse is logically equivalent to the inverse.
- p **only if** q means "if p then q".
- Biconditional: "if and only if" is true if both statements have the same value.

2.2.1 Necessary and Sufficient Conditions

- r is a sufficient condition for s means "if r then s"
- r is a necessary condition for s means "if not r then not s"

2.3 Valid and Invalid Arguments

2.3.1 Arguments Terminology

- **Argument**: sequence of statements
- All statements in an argument except for the final one are called premises
- The final statement is called a conclusion.
- An argument form being valid means that if the resulting premises are all true, the conclusion is true.
- **Critical row**: role of the truth table in which all premises are true. If the conclusion in every critical row is true, the argument form is valid.
- **Syllogism**: argument form consisting of two premises and a conclusion. The first and second premises in a syllogism are the major and minor premises respectively.

- **Modus ponens**: If p then q. p. $\therefore q$. Modus ponens means "method of affirming" in Latin.
- **Modus tollens**: If p then q. $\sim q, \therefore \sim p$. Modus tollens means "method of denying" in Latin.

2.3.2 Rule of Inference

Rule of Inference: form of argument that is valid. Below are some helpful Rules of Inference.

- **Generalization**: $p \therefore p \vee q$
- **Specialization**: $p \wedge q \therefore p$
- **Elimination**: $p \vee q, \sim q \therefore p$
- **Transitivity**: $p \to q, q \to r \therefore p \to r$
- **Proof by casework**: $p \vee q, p \to r, q \to r \therefore r$

2.3.3 Fallacies

- Using ambiguous premises
- Assuming that is to be proved
- Jumping to a conclusion
- Assuming the converse to be true.
- Assuming the inverse to be true.
- An argument is sound if and only if it is valid and all its premises are true.

2.3.4 Contradiction Rule

$\sim p \to c \therefore p$, in other words, if you can prove that an assumption leads to a contradiction, then you have proved that the assumption is false.

Chapter 3

The Logic of Quantified Statements

3.1 Predicates and Quantified Statements I

3.1.1 Terminology

- **Predicate Calculus**: Symbolic analysis of predicates and quantified statements
- **Statement Calculus**: Symbolic analysis of ordinary compound statements (see Sections 2.1-2.3)
- **Predicate**: part of the sentence from which the subject has been removed. A predicate is a predicate symbol together with predicate variables. Predicates become statements when specific values are substituted for the variables.
  - Note that predicates can be obtained by removing some or all the nouns from a statement.
- **Predicate symbols**: variables to stand for predicates that act as functions that take in predicate variables
- **Domain of a predicate variable**: set of all values that may be substituted in place of the variable.
- **Truth set of $P(x)$**: set of all elements of D that make $P(x)$ true when they are substituted for x.

$$\{x \in D \mid P(x)\}.$$

3.1.2 The Universal Quantifier: $\forall$

Definition 1: Universal Statement

Let $Q(x)$ be a predicate and D the domain of x. A **universal statement** (statement of the form $\forall x \in D, Q(x)$) is true if, and only if, $Q(x)$ is true for every x in D. It is false if there is a counterexample.

One way to show that a universal statement is true is by showing that there are no counterexamples. This is called the **method of exhaustion**.

3.1.3 The Existential Quantifier: $\exists$

Definition 2: Existential Statement

Let $Q(x)$ be a predicate and D the domain of x. An **existential statement** (statement of the form $\exists x \in D, Q(x)$) is true if, and only if, $Q(x)$ is true for at least one x in D. It is false if and only if $Q(x)$ is false for all x in D.

3.1.4 Equivalent Forms of Universal and Existential Statements

Observe that ($\forall x \in U$, if $P(x)$ then $Q(x)$) can always be rewritten as $\forall x \in D, Q(x)$ by narrowing U to be the domain D where D consists of all values x that make $P(x)$ true.

3.1.5 Implicit Quantification

Definition 3: Implication Notation

Let $P(x)$ and $Q(x)$ be predicates.

- $P(x) \implies Q(x) \equiv \forall x, P(x) \to Q(x)$, meaning every element in the truth set of $P(x)$ is also in the truth set of $Q(x)$.
- $P(x) \Leftrightarrow Q(x) \equiv \forall x, P(x) \leftrightarrow Q(x)$, meaning the two predicates have identical truth sets.

3.2 Predicates and Quantified Statements II

This section contains rules for negating quantified statements and additional extensions to quantified statements.

Theorem 1: Negation of a Universal Statement

$$\sim(\forall x \in D, Q(x)) \equiv \exists x \in D \mid \sim Q(x).$$

In other words, the negation of a universal statement is that there exists a counterexample.

Theorem 2: Negation of an Existential Statement

$$\sim(\exists x \in D \mid Q(x)) \equiv \forall x \in D, \sim Q(x).$$

In other words, the negation of an existential statement is the universal statement "none are" or "all are not".

Note that using the Negation of a Universal Statement theorem, we can find the negation of a universal conditional statement by negating the quantifier and the conditional "separately".

$$\sim(\forall x, P(x) \to Q(x)) \equiv \exists x \mid P(x) \land \ Q(x).$$

3.2.1 Relation among $\forall, \exists, \land, \lor$

Note that

$$\forall x \in D, Q(x) \equiv Q(x_1) \land Q(x_2) \land \ldots \land Q(x_n).$$

Similarly,

$$\exists x \in D \mid Q(x) \equiv Q(x_1) \lor Q(x_2) \lor \ldots \lor Q(x_n).$$

Using this, we can easily prove the above two theorems using DeMorgan's Laws. Additionally, note that contrapositives, converses, and inverses extend to universal conditional statements as well, and there is no need to flip the quantifier when finding these.

3.2.2 Necessary and Sufficient Conditions

Definition 4: Sufficient/Necessary Conditions

- "$\forall x, r(x)$ is a **sufficient condition** for $s(x)$" means "$\forall x, r(x) \to s(x)$".
- "$\forall x, r(x)$ is a **necessary condition** for $s(x)$" means "$\forall x, \sim r(x) \to \sim s(x)$".

3.3 Statements with Multiple Quantifiers

When there are multiple quantifiers, we perform the quantifiers in the order that they are stated. In terms of coding, it may be helpful to think of the first quantifier as the outer loop and the second quantifier as the inner loop in a case with 2 quantifiers. Amazingly, note that the order of the quantifiers only matters between $\forall$ and $\exists$.

3.3.1 Negations of Multiply-Quantified Statements

We simply negate the statement from left to right.

$$\sim(\forall x \in D, \exists y \in E \mid P(x,y)) \tag{3.1}$$
$$\equiv \exists x \in D \mid \sim(\exists y \in E \mid P(x,y)) \tag{3.2}$$
$$\equiv \exists x \in D \mid \forall y \in E, \sim P(x,y) \tag{3.3}$$

3.4 Arguments with Quantified Statements

Definition 5: Rule of Universal Instantiation

If some property is true of *everything* in a set, then it is true of *any particular* thing in the set.

3.4.1 Universal Modus Ponens/Tollens

Rule of Universal Instantiation can be used in combination with Modus Ponens in order to establish that a universal conditional statement can establish that the necessary condition necessarily follows from the sufficient condition. Forms of Modus Ponens and Modus Tollens can be found in Section 2.3.1.

3.4.2 Disc Diagrams

They're basically inheritance diagrams. Since I don't know how to draw with LaTeX yet, just check 3.4.5 of the book for more info.

3.4.3 Universal Transitivity

Definition 6: Universal Transitivity

If $\forall x P(x) \to Q(x), Q(x) \to R(x)$, then $\forall x P(x) \to R(x)$.

Chapter 4

Elementary Number Theory and Methods of Proof

4.1 Direct Proof and Counterexample I: Introduction

Definition 7: Even and Odd

An integer n in **even** if, and only if, n equals twice some integer. An integer n is **odd** if, and only if, n equals twice some integer plus 1.

Definition 8: Prime and Composite

An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$ then either r or s equals n. An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

4.1.1 Proving Existential Statements

There are two ways to prove an existential statement: find one condition that satisfies the predicate, or give a set of directions for finding that condition. These methods are called **constructive proofs of existence**. A **nonconstructive proof of existence** shows that the condition satisfying the predicate is guaranteed from some axiom/theorem, or showing that the lack of such a condition would lead to a contradiction.

4.1.2 Disproving Universal Statements

Definition 9: Disproof by Counterexample

To disprove a universal statement of the form $\forall x \in D, P(x) \to Q(x)$, simply find an x for which $P(x)$ is true and $Q(x)$ is false.

4.1.3 Proving Universal Statements

The **Method of Exhaustion**, although impractical, can work for small domains. For more general cases, we use

Definition 10: Method of Generalizing from the Generic Particular

To show that every element of a set satisfies a certain property, show that a particular but arbitrary chosen x satisfies the property. When using this method on a universal conditional, this is known as the **method of direct proof**.

Definition 11: Existential Instantiation

If the existence of a certain kind of object is assumed or has been deduced then it can be given a name, as long as that name is not currently being used to denote something else.

4.1.4 Proof Guidelines

1. Copy the statement of the theorem to be proved on your paper.
2. Clearly mark the beginning of your proof with the word **Proof**.
3. Make your proof self-contained.
4. Write your proof in complete, grammatically correct sentences.
5. Keep your reader informed about the status of each statement in your proof.
6. Give a reason for each assertion in your proof.
7. Include the "little words and phrases" that make the logic of your arguments clear.
8. Display equations and inequalities.
9. Note: be careful with using the word if. Use because instead if the premise is not in doubt.

4.1.5 Disproving Existential Statements

In order to prove that an existential statement is false, you simply have to prove that its negation is true.

4.2 Direct Proof and Counterexample II: Rational Numbers

Definition 12: Rational Number

A real number is **rational** if, and only if, it can be expressed as a quotient of two integers with a nonzero denominator. A real number that is not rational is **irrational**.

Theorem 3: Rational Number Properties

- Every integer is a rational number.
- The sum of any two rational numbers is rational.

Definition 13: Corollary

A statement whose truth can be immediately deduced from a theorem that has already been proven.

4.3 Direct Proof and Counterexample III: Divisibility

Definition 14: Divisibility

If n and d are integers and $d \neq 0$ then n is **divisible by** d if, and only if, n equals d times some integer. The notation $d \mid n$ is read "d divides n". Symbolically,

$$d \mid n \leftrightarrow \exists k \in \mathbb{Z} \mid n = dk.$$

It then follows that

$$d \nmid n \leftrightarrow \forall k \in Z | n \neq dk.$$

4.3.1 The Unique Factorization of Integers Theorem

Because of its importance, this theorem is also called the *fundamental theorem of arithmetic*. It states that any integer greater than 1 either is prime or can be written as a product of prime numbers in a way that is unique. Formally,

Theorem 4: Unique Factorization of Integers

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

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

When the values of p are ordered in non decreasing order, the above is known as the **standard factored form** of n.

4.4 Direct Proof and Counterexample IV: Division into Cases and the Quotient-Remainder Theorem

Theorem 5: The Quotient-Remainder Theorem

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

$$n = dq + r, 0 \leq r < d.$$

Note that if n is negative, the remainder is still positive.

4.4.1 div and mod

From the quotient remainder theorem, div is the value q, and mod is the value r. Note that

$$n \; mod \; d = n - d \cdot (n \; div \; d).$$

4.4.2 Method of Proof by Division into Cases

To prove a statement of the form "If A_1 or A_2 or A_3 or ... or A_n, then C prove that A_i for all $1 \leq i \leq n$ implies C. This is useful when a statement can be easily split into multiple statements that fully encompass the original statement.

Example 1

Prove that the square of any odd integer has the form $8m + 1$ for some integer m.

Proof (Brief). Suppose n is an odd integer. By the quotient remainder theorem and using the fact that the integer is odd, we can split the possible forms of n into two cases: $4q + 1$ or $4q + 3$ for some integer q. It can be proven through substitution that these two cases simplify to the form $n^2 = 8m + 1$.

4.4.3 Absolute Value and the Triangle Inequality

Definition 15: Absolute Value

For any real number x, the **absolute value of x** is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} \tag{4.1}$$

Theorem 6: Triangle Inequality

For all real numbers x and y, $|x + y| \leq |x| + |y|$.

4.5 Indirect Argument: Contradiction and Contraposition

Proof by contradiction is extremely intuitive and exactly what it sounds like. Assume that the negation is true, and show that this assumption leads to a contradiction. Argument by contrapositive is equally intuitive given the fact that a statement is logically equivalent to its contrapositive. Note that proof by contraposition can only be used on universal conditionals.

Chapter 5

Sequences, Mathematical Induction, and Recursion

The proof chapter is finally over! I did not like that chapter D:

5.1 Sequences

Definition 16: Sequence

A **sequence** is a function whose domain is either all the integers between two given integers or all the integers greater than or equal to a given integer.

The first term of a sequence is known as the **initial term**, and the last term is known as the **final term**. An **explicit formula** or **general formula** is a rule that shows how the values of a_k depend on k.

5.1.1 Summation Notation

Definition 17: Summation Notation

For integers m and n where $m \leq n$,

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \ldots + a_n.$$

We call k the **index** of the summation, m the **lower limit** of the summation, and n the **upper limit** of the summation.
A recursive definition of summation notation:

$$\sum_{k=m}^{m} a_k = a_m \text{ and } \sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n.$$

5.1.2 Product Notation

Definition 18: Product Notation

For integers m and n where $m \leq n$,

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot \ldots \cdot a_n.$$

The recursive definition of product notation is in essence the same idea as the one in summation notation.

5.1.3 Properties of Summations and Products

Theorem 7: Properties

1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$
2. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$
3. $(\prod_{k=m}^{n} a_k) * (\prod_{k=m}^{n} b_k) = (\prod_{k=m}^{n} (a_k \cdot b_k))$

Substituting a new variable for k is simple. Change the limits by setting k equal to each of the limits and noting the new value, then change the expression itself by substituting k.

5.2 Mathematical Induction

The general structure of mathematical induction mirrors a line of thinking somewhat like a domino effect: If we can show that some property $P(n)$ is true for some integer a, and for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true, then the statement "for all integers $n \geq a, P(n)$ is true. This is known as the **Principle of Mathematical Induction**. Showing that $P(n)$ is true for some integer a is known as the **basis step**, and proving that the truth of $P(k+1)$ follows from the truth of $P(k)$ is known as the **inductive step**.

Example 2: Sum of the First n Integers

For all integers $n \geq 1$,

$$1 + 2 + \ldots + n = \frac{n * (n+1)}{2}.$$

Proof (Brief). Let the property $P(n)$ be the given equation. It can be shown that $P(1)$ is true. We assume that $P(k)$ is true ($P(k)$ is known as the **inductive hypothesis**) and use the fact that $P(k) + k = P(k+1)$. Using algebraic manipulation, we find that $P(k+1)$ is true.

In general, use the inductive hypothesis to prove the inductive step.

5.3 Strong Mathematical Induction

Definition 19: Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a), P(a+1), \ldots, P(b)$ are all true. (**basis step**)
2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. (**inductive step**)

Then the statement

$$\text{for all integers } n \geq a, P(n).$$

is true.

Example 3: Number of Multiplications Needed to Multiply n Numbers

Prove that for any integer $n \geq 1$, if $x_1, x_2, \ldots x_n$ are n numbers, then no matter how the parentheses are inserted into their product, the number of multiplications used to compute the product is $n-1$.

Proof (Brief). $P(1)$ is evidently true, as it takes 0 multiplications to multiply one number. Using the inductive hypothesis that $P(i)$ is true for all integers i from 1 to k, we now attempt to prove that $P(k+1)$ is also true. We do this by splitting the $k+1$ integers into two sides with l $(1 \leq l \leq k)$ factors on the left and r $(1 \leq r \leq k)$ factors on the right.

By inductive hypothesis, we note that we end up with $(l-1)+(r-1)+1 = l+r-1$ multiplications, which, when considering that $l+r = k+1$, proves the statement.

Definition 20: Well-Ordering Principle for the Integers

Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element.

A consequence of the well-ordering principle is the fact that any strictly decreasing sequence of nonnegative integers is finite. (This is because from the well-ordering principle, there must be some least element r_k, which is the final element, because if there were some term r_{k+1}, then $r_{k+1} < r_k$, which contradicts the well-ordering principle.

5.4 Recursion

Solving a problem recursively means to find a way to break it down into smaller subproblems each having the same form as the original problem.

Example 4: Tower of Hanoi

What is the least number of steps to move 64 golden disks from pole A to pole C (given the information that there are three poles, all the disks are different sizes, and at any point, discs on every pole must be in increasing order of size)?

The key observation here is to note that if we know the solution for $k-1$ discs, we can use this information to get the solution for k discs:

1. Move $k-1$ discs to pole B.
2. Move the bottom disc of pole A to pole C.
3. Move all the discs from pole B to pole C.

It then follows that we get the recurrence $m_k = 2m_{k-1} + 1$ where m_k is the number of moves to move k discs from one pole to another.

An explicit formula for this recurrence can be found through iteration and using the formula for the sum of a geometric sequence. From this, we get the formula $m_n = 2^n - 1$.

5.4.1 Checking the Correctness of Explicit Formulas

We can use mathematical induction to check the correctness of explicit formulas. For example, we can verify the formula for Tower of Hanoi by showing that it is true for 1 ring, and then showing that it is true for all $k+1$ assuming that k is true. Check your induction proof carefully to make sure that no mistakes were made, and that the recursive form as well as the explicit form were both used.

Chapter 6

Set Theory

All mathematical objects can be defined in terms of sets, and the language of set theory is used in every mathematical subject.

6.1 Definitions and the Element Method of Proof

Sets, as defined earlier, are collections of objects, called elements. Using our new knowledge, we can redefine some definitions.

6.1.1 Subsets

We can redefine some definitions of subsets:

$$A \subseteq B \Leftrightarrow \forall x, x \in A \rightarrow x \in B.$$

$$A \not\subseteq B \Leftrightarrow \exists x \mid x \in A \wedge x \notin B.$$

Recall that a **proper subset** is a subset that is not equal to its containing set.

We can prove for two sets X and Y that $X \subseteq Y$ by **supposing** that x is a particular but arbitrarily chosen element of X, and **showing** that x is also an element of Y.

Definition 21: Set Equality

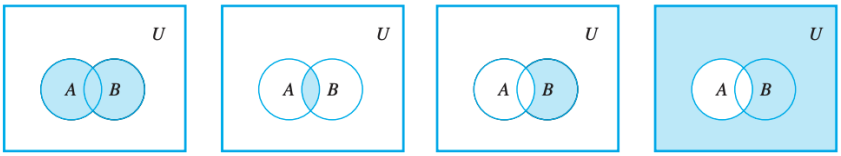
Set A equals set B if, and only if, $A \subseteq B$ and $B \subseteq A$.

6.1.2 Operations on Sets

Definition 22: Operations

Let A and B be subsets of a universal set U.

1. The **union** of A and B, denoted $A \cup B$, is the set of all elements that are in at least one of A or B.
2. The **intersection** of A and B, denoted $A \cap B$, is the set of all elements that are common to both A and B.
3. The **difference** of B minus A (or **relative complement** of A in B), denoted $B - A$, is the set of all elements that are in B and not A.
4. The **complement** of A, denoted A^c, is the set of all elements in U that are not in A.



Shaded region represents $A \cup B$. | Shaded region represents $A \cap B$. | Shaded region represents $B - A$. | Shaded region represents A^c.

6.1.3 Disjoint Sets and Partitions

A group of sets are **mutually disjoint** if the intersection of all pairs of sets is equal to the empty set $\emptyset$.

Definition 23: Partition

A finite or infinite collection of nonempty sets $\{A_1, A_2, A_3 \ldots\}$ is a **partition** of a set A if, and only if,

1. A is the union of all the A_i
2. The sets $A_1, A_2, A_3 \ldots$ are mutually disjoint.

Definition 24: Power Sets

Given a set A, the **power set** of A, denoted $\wp(A)$, is the set of all subsets of A.

Definition 25: Cartesian Product

In general,

$$A_1 \times A_2 \times \ldots A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Note that $A_1 \times A_2 \times A_3$ is not quite the same thing as $(A_1 \times A_2) \times A_3$ because of tuple ordering.

6.2 Properties of Sets

Theorem 8: Some Subset Relations

1. Inclusion of Intersection: $A \cap B \subseteq A$ and vice versa
2. Inclusion in Union: $A \subseteq A \cup B$ and vice versa
3. Transitive Property of Subsets: $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$

To prove these theorems, *suppose* that there is some arbitrary element of A and show that it is also in B.

Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws:* For all sets A and B,
$$\text{(a) } A \cup B = B \cup A \quad \text{and} \quad \text{(b) } A \cap B = B \cap A.$$
2. *Associative Laws:* For all sets A, B, and C,
$$\text{(a) } (A \cup B) \cup C = A \cup (B \cup C) \quad \text{and}$$
$$\text{(b) } (A \cap B) \cap C = A \cap (B \cap C).$$
3. *Distributive Laws:* For all sets, A, B, and C,
$$\text{(a) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and}$$
$$\text{(b) } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
4. *Identity Laws:* For all sets A,
$$\text{(a) } A \cup \emptyset = A \quad \text{and} \quad \text{(b) } A \cap U = A.$$
5. *Complement Laws:*
$$\text{(a) } A \cup A^c = U \quad \text{and} \quad \text{(b) } A \cap A^c = \emptyset.$$
6. *Double Complement Law:* For all sets A,
$$(A^c)^c = A.$$
7. *Idempotent Laws:* For all sets A,
$$\text{(a) } A \cup A = A \quad \text{and} \quad \text{(b) } A \cap A = A.$$
8. *Universal Bound Laws:* For all sets A,
$$\text{(a) } A \cup U = U \quad \text{and} \quad \text{(b) } A \cap \emptyset = \emptyset.$$
9. *De Morgan's Laws:* For all sets A and B,
$$\text{(a) } (A \cup B)^c = A^c \cap B^c \quad \text{and} \quad \text{(b) } (A \cap B)^c = A^c \cup B^c.$$
10. *Absorption Laws:* For all sets A and B,
$$\text{(a) } A \cup (A \cap B) = A \quad \text{and} \quad \text{(b) } A \cap (A \cup B) = A.$$
11. *Complements of U and $\emptyset$:*
$$\text{(a) } U^c = \emptyset \quad \text{and} \quad \text{(b) } \emptyset^c = U.$$
12. *Set Difference Law:* For all sets A and B,
$$A - B = A \cap B^c.$$

In general, to prove set equality, you prove that set A is a subset of set B, and that set B is a subset of set A. Additionally, to prove that a set X is equal to the empty set $\emptyset$, suppose X has an element and derive a contradiction.

Additionally, casework is helpful when dealing with unions. It may be helpful to split a union into 2 cases.

Chapter 7

Functions

In this chapter we go more in depth into properties of functions and their composition.

7.1 Functions Defined on General Sets

Definition 26: Function

A **function** from a set X to a set Y, denoted $f : X \to Y$, is a relation from X, the **domain**, to Y, the **co-domain**, that satisfies two properties:

1. Every element in X is related to some element in Y
2. No element in X is related to more than one element in Y.

The set of all values of f is called the *range of* f or the *image of* X *under* f. If there exists some x such that $f(x) = y$, then x is called a **preimage (or inverse image) of** y.
Two functions $F : X \to Y$ and $G : X \to Y$ are considered equal if, for all $x \in X, F(x) = G(x)$

Definition 27: Identity Function

The identity function I_X is a function from $X \to X$ by which $I_X(x) = x \forall x \in X$.

Definition 28: Logarithmic Function

The log function $\log_b x = y$ (from $\mathbb{R}^+$ to $\mathbb{R}$) maps a number to the y in the solution of the equation $b^y = x$.

7.1.1 Well Defined Functions

We say that a function is **not well defined** if it fails to satisfy at least one of the requirements for being a function. A function being well defined really

means that it qualifies to be called a function.

7.2 One-to-One and Onto, Inverse Functions

7.2.1 One-to-one

A function is **one-to-one** (or **injective**) if, and only if, every input has a unique output. Symbolically, $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \to x_1 = x_2$.

To prove that f is one-to-one, you **suppose** x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$, and **show** that $x_1 = x_2$.

7.2.2 Onto

A function is **onto** (or **surjective**) if, and only if, the co-domain of the function is equal to its image. Symbolically, $\forall y \in Y, \exists x \in X \mid f(x) = y$.

To prove that f is onto, you **suppose** y is in Y, and **show** that there exists an element in x such that $y = f(x)$.

7.2.3 One-to-one correspondences and Inverse Functions

Definition 29: Bijection

A **one-to-one correspondence** (or **bijection**) from a set X to a set Y is a function that is both one-to-one and onto.

Theorem 9: Inverse Functions

Suppose $F : X \to Y$ is a one-to-one correspondence. Then there is a function $F^{-1} : Y \to X$ where $F^{-1}(y) = x$. Note that F^{-1} is also a one-to-one correspondence.
Additionally, note that

$$f^{-1}(b) = a \Leftrightarrow f(a) = b.$$

Finding an inverse function is done while proving that some function F is onto.

7.3 Composition of Functions

The composition of functions (defined as $(g \circ f)(x) = g(f(x)) \forall x \in X$) for two functions $f : X \to Y$ and $g : Y \to Z$ is $(g \circ f) : X \to Z$. Two compositions are equivalent if they have the same output for every input.

Theorem 10: Composition of a Function with Its Inverse

$f^{-1} \circ f = I_X$ and $f \circ f^{-1} = I_Y$. This can be proved directly using the definition of inverse.

Theorem 11: One-to-one/Onto Compositions

If $f : X \to Y$ and $g : Y \to Z$ are both one-to-one, then $g \circ f$ is one-to-one. The same line of reasoning applies for onto functions.

7.4 Cardinality and Sizes of Infinity

Definition 30: Cardinality

Let A and B be any sets. A **has the same cardinality as** B if, and only if, there is a one-to-one correspondence from A to B. Sets in terms of cardinality follow reflexive, symmetric, and transitive properties.

Note that if a set has the same cardinality as a set that is countably infinite, then the set is also countably infinite. Surprisingly, the set of all rational numbers is countably infinite.

7.4.1 Larger Infinities

The set of all real numbers is uncountable. This can be proved using the Cantor diagonalization process. Note that any subset of a countable set is countable, and any subset with an uncountable set is uncountable.