MATH 3325

Jay Melendez

August 2021

Contents

This is a compilation of notes (a lot of them verbatim or at least paraphrased) taken from:

- A Transition to Advanced Mathematics; Smith, Eggen, Andre
- Book of Proof; Hammack
- Professor Alan Haynes Math 3338 - Probability Course Handouts
- Statistical Inference; Casella, Berger

Most of this is the work of smart people, not me. The things that are wrong are probably from me.

1 Logic

1.1 Propositions and Connectives

A **proposition** is a sentence that has exactly one truth value: **true**, denoted by **T**, or **false**, denoted by **F**.

The **negation** of a proposition P, denoted $\neg P$, is the proposition "not P." The proposition $\neg P$ is true when P is false.

Definition 1.1.1. Given propositions P and Q, the **conjunction** of P and Q, denoted $P \wedge Q$, is the proposition "P and Q." $P \wedge Q$ is true exactly when *both* P and Q are true.

P	**Q**	**P** $\wedge$ **Q**
T	T	T
T	F	F
F	T	F
F	F	F

Definition 1.1.2. Given propositions P and Q, the **disjunction** of P and Q, denoted $P \vee Q$, is the proposition "P or Q." $P \vee Q$ is true exactly when *at least one of* P or Q is true.

P	**Q**	**P** $\vee$ **Q**
T	T	T
T	F	T
F	T	T
F	F	F

Definition 1.1.3. A **tautology** is a propositional form that is true for *every* assignment of truth values to its components.

P	**Q**	**P** $\vee$ **Q**	$\neg$**P**	$\neg$**Q**	$\neg$**P** $\wedge$ $\neg$**Q**	(**P** $\vee$ **Q**) $\vee$ ($\neg$**P** $\wedge$ $\neg$**Q**)
T	T	T	F	F	F	T
F	T	T	T	F	F	T
T	F	T	F	T	F	T
F	F	F	T	T	T	T

Two propositional forms are **equivalent** if and only if they have the same truth tables.

P	$\neg$**P**	$\neg$($\neg$**P**)
T	F	T
F	T	F

Note that P s equivalent to $\neg(\neg P)$.

Theorem 1.1.1. For propositions P, Q, and R, the following are equivalent:

P	$\equiv$	$\neg P$	**Double Negation Law**
$P \vee Q$	$\equiv$	$Q \vee P$	**Commutative Laws**
$P \wedge Q$	$\equiv$	$Q \wedge P$	**Commutative Laws**
$P \vee (Q \vee R)$	$\equiv$	$(P \vee Q) \vee R$	**Associative Laws**
$P \wedge (Q \wedge R)$	$\equiv$	$(P \wedge Q) \vee R$	**Associative Laws**
$P \wedge (Q \vee R)$	$\equiv$	$(P \wedge Q) \vee (P \wedge R)$	**Distributive Laws**
$P \vee (Q \wedge R)$	$\equiv$	$(P \vee Q) \wedge (P \vee R)$	**Distributive Laws**
$\neg(P \wedge Q)$	$\equiv$	$\neg P \vee \neg Q$	**De Morgan's Laws**
$\neg(P \vee Q)$	$\equiv$	$\neg P \wedge \neg Q$	**De Morgan's Laws**

1.2 Conditionals and Biconditionals

Definition 1.2.1. For propositions P and Q, the **conditional sentence** $P \Rightarrow Q$ is the proposition "If P, then Q." Proposition P is called the **antecedent** and Q is called the **consequent**. The conditional sentence $P \Rightarrow Q$ is true *if and only if* P is false or Q is true. Conversely, $P \Rightarrow Q$ is false *only* when P is true and Q is false.

P	**Q**	**P $\Rightarrow$ Q**
T	T	T
T	F	T
F	T	F
F	F	T

Note: By the rule of **Material Implication**, $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$.

Theorem 1.2.1. Let P and Q be propositions.

The **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$	Not Equivalent to $P \Rightarrow Q$
The **contrapositive** is $(\neg Q) \Rightarrow (\neg P)$	Equivalent to $P \Rightarrow Q$.

Definition 1.2.2. For propositions P and Q, the **biconditional sentence** $P \Leftrightarrow Q$ is the proposition "P *if and only if* Q." $P \Leftrightarrow Q$ is true exactly when P and Q have the *same* truth values. We also write P iff Q to abbreviate "P if and only if Q.

P	**Q**	**P $\Leftrightarrow$ Q**
T	T	T
T	F	F
F	T	F
F	F	T

Note: $P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$.

Theorem 1.2.2. For propositions P, Q, and R,

$$\begin{array}{lcl} P \Rightarrow Q & \equiv & \neg P \vee Q \\ \neg(P \Rightarrow Q) & \equiv & P \wedge \neg Q \\ \neg(P \wedge Q) & \equiv & P \Rightarrow \neg Q \\ & \equiv & Q \Rightarrow \neg P \\ P \Rightarrow (Q \Rightarrow R) & \equiv & (P \wedge Q) \Rightarrow R \\ P \Rightarrow (Q \wedge R) & \equiv & (P \Rightarrow Q) \wedge (P \Rightarrow R) \\ (P \vee Q) \Rightarrow R & \equiv & (P \Rightarrow R) \wedge (Q \Rightarrow R) \\ P \Leftrightarrow Q & \equiv & (P \Rightarrow Q) \wedge (Q \Rightarrow P). \end{array}$$

1.3 Quantifiers

A sentence that contains variables (e.g., "$x \geq 3$") is considered an **open sentence** or **predicate** until its variables are assigned specific values. When P is an open sentence with a variable x, the predicate is symbolized by $P(x)$.

Before the *truth* value can be determined, we must take into account *where this predicate lives* in order to decide what objects are available to satisfy the predicate's conditions.

Definition 1.3.1. The **Universe of Discourse** must be established. The universe determines what objects are available to use in order to satisfy the predicate's requirements. Number systems are often used to denote the universe, (these are familiar):

$\mathbb{N}$	$= \{1, 2, 3, ...\}$,	The set of **Natural Numbers**
$\mathbb{Z}$	$= \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$	The set of **Integers**
$\mathbb{Q}$	$= \{\ p/q \mid p, q \in \mathbb{Z}\}$	The set of **Rational Numbers**
$\mathbb{R}$	$= \{x \mid x \in \mathbb{Q}\ or\ x \in \mathbb{I}\}$	The set of all **Real Numbers**
$\mathbb{I}$	$= \{x \mid x \in \mathbb{R}\ and\ x \notin \mathbb{Q}\}$	The set of all **Real Numbers**
$\mathbb{C}$	$= \{a + bi \mid a, b \in \mathbb{R}\ and\ i = \sqrt{-1}\}$	The set of **Complex Numbers**

Definition 1.3.2. For a predicate, $P(x)$, the sentence $(\exists x)P(x)$ is read "There *exists* x such that $P(x)$" or- "For some x, $P(x)$." The sentence $(\exists x)P(x)$ is true if there is at least *one* case that can be established where x exists. The symbol $\exists$ is called the **Existential Quantifier.**

Definition 1.3.3. For a predicate $P(x)$, the sentence $(\forall x)P(x)$ is read "For all x, $P(x)$ and is true iff x is true for the *entire* universe. The symbol $\forall$ is called the **Universal Quantifier**.

There are many ways to express a quantified sentence. Look for keywords such as: for all," "for every," "for each," "some," "at least one," "there exist(s)," etc. For example, someone who says "Polynomial functions are continuous" means that "All polynomial functions are continuous." Yet someone who says "Rational functions have vertical asymptotes" must mean: "Some rational functions have vertical asymptotes."

Generally:
A sentence of the form "All $P(x)$ are $Q(x)$" should be symbolized:

$$(\forall x)[P(x) \Rightarrow Q(x)].$$

A sentence of the form "Some $P(x)$ are $Q(x)$" should be symbolized:

$$(\exists x)[P(x) \wedge Q(x)].$$

Examples.

Sentence: For every odd prime x less than 10, $x^2 + 4$ is prime.

Implications: If x is prime, and odd, and less than 10, then $x^2 + 4$ is prime.

Quantified: $(\forall x)[[(x \text{ is prime}) \wedge (x \text{ is odd}) \wedge (x < 10)] \Rightarrow (x^2 + 4 \text{ is prime})]$.

Sentence: Some real numbers have a multiplicative inverse.

Implications: There is an $x \in \mathbb{R}$ and x has a multiplicative inverse. *Note* that since x has an inverse, this implies there exists another number, y, that is an inverse for x, therefore this predicate possesses a hidden quantifier.

Quantified: $(\exists x)[x \in \mathbb{R} \wedge (\exists y)(y \in \mathbb{R} \wedge xy = 1)]$.

Sentence: Some integers are even and some integers are odd.

Implications: The first quantifier will only extend as far as the word "even", so it would be preferable to show this as two separate variables, x and y. *Note*: There will need to be TWO quantifiers used, as one number cannot exist as both even and odd.

Quantified: $(\exists x)(x \text{ is even}) \wedge (\exists y)(y \text{ is odd})$. -or- $(\exists x)(x = 2k) \wedge (\exists y)(y = 2k + 1)$.

Sentence: Every element of the set A has property P.

Quantified: $(\forall x \in A)P(x)$.

Sentence: Some element in the set A has property P.

Quantified: $(\exists x \in A)P(x)$.

Theorem 1.3.1. If $A(x)$ is an open sentence with variable x, then:

$$\neg(\forall x)A(x) \equiv (\exists x)\neg A(x)$$
$$\neg(\exists x)A(x) \equiv (\forall x)\neg A(x)$$

Proof. To show $\neg(\forall x)A(x) \equiv (\exists x)\neg A(x)$:

Let U be *any* universe.
The sentence $\neg(\forall x)(A(x)$ is true in U
iff $(\forall x)A(x)$ is false in U
iff the truth set of $A(x)$ is not in the universe
iff the truth set of $\neg A(x)$ is nonempty
iff $(\exists x)\neg A(x)$ is true in U. □

Example. For the universe of all real numbers, find a denial of "Every positive real number has a multiplicative inverse."

Note: There is a hidden quantifier in this proposition. For x to have a multiplicative inverse, there must be a y such that $xy = 1$.

Symbolized:

$$\forall x[x > 0 \Rightarrow (\exists y)(xy = 1)]$$

Negation:

$$\begin{aligned}
&\neg\, \forall x[x > 0 \Rightarrow (\exists y)(xy = 1)] \\
&\equiv \exists x \,\neg\, [x > 0 \Rightarrow (\exists y)(xy = 1)] \\
&\equiv \exists x \,\neg\, [\neg(x > 0) \vee (\exists y)(xy = 1)] \quad \text{material implication} \\
&\equiv \exists x[x > 0 \wedge \neg(\exists y)(xy = 1)] \\
&\equiv \exists x[x > 0 \wedge (\forall y) \,\neg\, (xy = 1)] \\
&\equiv \exists x[x > 0 \wedge (\forall y)(xy \neq 1)]
\end{aligned}$$

This last sentence may be translated as "There is a positive real number that has no multiplicative inverse."

1.4 Rules of Inference

Suppose we know that a conditional statement $P \Rightarrow Q$ is true. This tells us that whenever P is true, Q will also be true. By itself, $P \Rightarrow Q$ tells us nothing, because P could be false and Q true or false and it would still be yield the same truth value. However, if we happen to know that P is true, *then* Q *must* be true. This is called a **logical inference**. From two true statements we infer that a third statement is true. In essence, statements $P \Rightarrow Q$ and P are "added together" to get Q. We indicate this by stacking $P \Rightarrow Q$ and P one atop the other with a line separating them from Q. The intended meaning is that $P \Rightarrow Q$ combined with P produces Q.

Modus Ponens

$$\begin{array}{l} P \Rightarrow Q \\ P \\ \hline Q \end{array}$$

Modus Tollens

$$\begin{array}{l} P \Rightarrow Q \\ \neg Q \\ \hline \neg P \end{array}$$

Elimination

$$\begin{array}{l} P \vee Q \\ \neg P \\ \hline Q \end{array}$$

Note: Moving on to proofs, you will rarely be using logical symbols such as $\wedge, \vee, \exists$, or $\forall$. These just form the basis (or inner-workings) of mathematical proofs.

2 Basic Proof Methods

2.1 General Definitions / Parts of Mathematical Proofs

A **theorem** is a mathematical statement that is true and can (and has been) verified as true.

A **proof** of a theorem is a written verification that shows that the theorem is definitely and unequivocally true.

A **definition** is an exact, unambiguous explanation of the meaning of a mathematical word or phrase.

An **axiom** or *axioms* is an initial set of statements that are assumed to be true.

A **proposition** is a statement that is true but not as significant as a theorem.

A **lemma** is a theorem whose main purpose is to help prove another theorem.

A **corollary** is a result that is an immediate consequence of a theorem or proposition.

2.2 Mathematical Definitions for Proofs (Set 1)

Definition 2.2.1. An integer n is **even** if $n = 2k$ for some integer $k \in \mathbb{Z}$.

Definition 2.2.2. An integer n is **odd** if $n = 2k + 1$ for some integer $k \in \mathbb{Z}$.

Definition 2.2.3. Two integers have the **same parity** if they are both even or they are both odd. Otherwise they have **opposite parity.**

Definition 2.2.4. Suppose a and b are integers. We say that a **divides** b, written $a|b$, if $b = ac$ for some $c \in \mathbb{Z}$. In this case we also say that a is a **divisor** of b, and that b is a **multiple** of a.

Definition 2.2.5. A number $n \in \mathbb{N}$ is **prime** if it has exactly two positive divisors, 1 and n. If n has more than two positive divisors, it is called **composite**. (Thus n is composite if and only if $n = ab$ for $1 < a, b < n$.) **Note:** This definition implies 1 is neither prime nor composite.

Definition 2.2.6. The **greatest common divisor** of integers a and b, denoted $gcd(a, b)$, is the largest integer that divides both a and b. *Note:* $gcd(0, n) = n$.

The **least common multiple** of non=zero integers a and b, denoted $lem(a, b)$, is the smalled integer in $\mathbb{N}$ that is a multiple of both a and b.

Definition 2.2.7. The **Division Algorithm**: Given integers a and b with $b > 0$, there exist unique integers q and r for which $a = qb + r$ and $0 \leq r < b$.

Definition 2.2.8. Definitions of Number Systems:

$\mathbb{N}$	$= \{1, 2, 3, ...\}$,	The set of **Natural Numbers**
$\mathbb{Z}$	$= \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$	The set of **Integers**
$\mathbb{Q}$	$= \{\ p/q \mid p, q \in \mathbb{Z}\}$	The set of **Rational Numbers**
$\mathbb{R}$	$= \{x \mid x \in \mathbb{Q}\ or\ x \in \mathbb{I}\}$	The set of all **Real Numbers**
$\mathbb{I}$	$= \{x \mid x \in \mathbb{R}\ and\ x \notin \mathbb{Q}\}$	The set of all **Real Numbers**
$\mathbb{C}$	$= \{a + bi \mid a, b \in \mathbb{R}\ and\ i = \sqrt{-1}\}$	The set of **Complex Numbers**

2.3 Some Properties of Number Systems (Set 1)

2.3.1 The Natural Numbers

1. *Successor properties*
   1 is a natural number.
   Every natural number x has a unique successor $x + 1$.
   1 is not the successor of any natural number.

2. *Closure properties*
   The sum of two natural numbers is a natural number.
   The difference of two natural numbers is a natural number.
   The product of two natural numbers is a natural number.

3. *Associativity properties*
   For all $x, y, z \in \mathbb{N}, x + (y + z) = (x + y) + z$.
   For all $x, y, z \in \mathbb{N}, x(yz) = (xy)z$.

4. *Commutativity properties*
   For all $x, y \in \mathbb{N}, x + y = y + x$.
   For all $x, y \in \mathbb{N}, xy = yx$.

5. *Disributivity properties*
   For all $x, y, z \in \mathbb{N}, x(y + z) = xy + xz$.
   For all $x, y, z \in \mathbb{N}, (y + z)x = yx + zx$.

6. *Cancellation properties*
   For all $x, y, z \in \mathbb{N}, x + z = y + z$, then $x = y$.
   For all $x, y, z \in \mathbb{N}, xz = yz$, then $x = y$.

Theorem 2.3.1. The Fundamental Theorem of Arithmetic:
Every natural number larger than 1 is prime or can be expressed uniquely as a product of primes. If we list the prime factors in increasing order, then there is only one prime factorization: the primes and their exponents are uniquely determined.

2.3.2 The Integers

1. *Closure properties*
   The sum of two integers is an integer.
   The difference of two integers is an integer.
   The product of two integers is an integer.

2. *Associativity properties*
   For all $x, y, z \in \mathbb{Z}, x + (y + z) = (x + y) + z$.
   For all $x, y, z \in \mathbb{Z}, x(yz) = (xy)z$.

3. *Commutativity properties*
   For all $x, y \in \mathbb{Z}, x + y = y + x$.
   For all $x, y \in \mathbb{Z}, xy = yx$.

4. *Disributivity properties*
   For all $x, y, z \in \mathbb{Z}, x(y + z) = xy + xz$.
   For all $x, y, z \in \mathbb{Z}, (y + z)x = yx + zx$.

5. *Cancellation properties*
   For all $x, y, z \in \mathbb{Z}, x + z = y + z$, then $x = y$.
   For all $x, y, z \in \mathbb{Z}, if z \neq 0, xz = yz$, then $x = y$.

6. *For all* $x \in \mathbb{Z}$
   if $x < y$ and $z > 0, xy < yz$.

2.4 Direct Proofs

Proving statements of the form $P \Rightarrow Q$.
1. Begin by assuming that P is *true.*
2. Show this forces Q to be *true.*

Outline for Direct Proof–

Proposition: If P, then Q.
Proof. Suppose P.
$\vdots$
Therefore Q.

Strategies for developing a direct proof of a conditional sentence:

1. Determine preceisely the hyptheses (if any) and the antecedent and consequent.
2. Replace (if necessary) the antecedentwith a more usable equivalent.
3. Replace (if necessary) the consequent by something equivalent and more readily shown.

4. Beginning with the assumption of the antecedent, develop a chain of statements that leads to the consequent. Each statement in the chain must be deducible from its predecessors or other known results (corrolary, lemma, etc.).

Example 2.4.1. Theorem: Let x be an integer. Prove that if x is odd, then $x+1$ is even.
Proof: (Broken down)

Note: The theorem has the form $P \Rightarrow Q$, where P is "x is odd" and Q is "x+1 is even."

Let x be an integer.	Assume this hypothesis since its given in the statement.
Suppose x is odd.	Assume the antecedent P is true.
From the definition of odd,	Goal is to derive the consequent Q as our last step.
$x = 2k+1$ for some integer k.	This deduction is the replacement of P by an equivalent statement-the definition of "odd."
Then, $x+1 = (2k+1)+1$ for some integer k.	Replacement using an algebraic property of $\mathbb{N}$.
Since $(2k+1)+1 = 2k+2 = 2(k+1)$,	Algebraic equivalent
$x+1$ is the product of 2 and an integer.	Algebraic equivalent
Thus $x+1$ is even.	We have deduced Q.
Therefore, If x is an odd integer, then $x+1$ is even.	We conclude that $P \Rightarrow Q$.

Proof. Let x be an integer. Suppose x is odd. From the definition of odd, $x = 2k+1$ for some integer k. Then, $x+1 = (2k+1)+1$ for some integer k. Since $(2k+1)+1 = 2k+2 = 2(k+1)$, $x+1$ is the product of 2 and an integer. Thus $x+1$ is even. Therefore, If x is an odd integer, then $x+1$ is even. □

Example 2.4.2. Theorem: Let a, b, and c are integers. Prove that if a divides b and b divides c, then a divides c.
Proof: (Broken down)

Let a, b, and c be integers.	Assume the hypothesis is true.
Suppose a divides b and b divides c.	Antecedent is compound statement $a\|b \wedge b\|c$
Then $b = ak$ for some integer k, and $c = bm$ for some integer m.	Replace assumptions by equivalents Don't assume k and m are same integer
Therefore, $c = bm = (ak)m = a(km)$	To show that $a\|c$, write c as a multiple of a
Then c is a multiple of a.	If k and m are integers, then km is an integer.
Therefore, if $a\|b$ and $b\|c$, then $a\|c$.	Write the operations out, I'm just using a—c to save space.

Proof. Let a, b, and c be integers. Suppose a divides b and b divides c. Then $b = ak$ for some integer k and $c = bm$ for some integer m. Therefore, $c = bm = (ak)m = a(km)$, where km is an integer. Then c is a multiple of a. Therefore, if a divides b and b divides c, then a divides c. □

Example 2.4.3. Theorem: Suppose a, b, and c are integers. Prove that if a divides b and a divides c, then a divides $b - c$.
Proof (Broken down):

Suppose a, b, and c are integers.	
Suppose a divides b and a divides c.	
Then $b = an$ for some integer n	Use definition of *divides*
and $c = am$ for some integer m..	
Thus,	
$b - c = an - am = a(n - m)$.	
Since $n - m$ is an integer,	Using the fact that the difference of two
a divides $b - c$.	integers is an integer

Proof. Suppose a, b, and c are integers. Suppose a divides b and a divides c. Then $b = an$ for some integer n. Thus, $b - c = an - am = a(n - m)$. Since $n - m$ is an integer, a divides $b - c$. □

3 Set Theory

3.1 Basic Concepts of Set Theory

Definition 3.1.1. A **set** is simply a *collection* of things called **elements**.

Two sets are **equal** if and only if they contain exactly the same elements. So $\{2, 4, 6, 8\} = \{4, 2, 8, 6\}$, but $\{2, 4, 6, 8\} \neq \{2, 4, 6, 7\}$. Also:

$$\{..., -3, -2, -1, 0, 1, 2, 3, ...\} = \{0, -1, 1, -2, 2, -3, 3, ...\}$$

We let uppercase letters stand for sets. For example, let $A = \{2, 4, 6, 8\}$. If some '*thing*' is part of a set, we say "2 is an *element* of A, or $2 \in A$. If some '*thing*' is not part of a set, we say "5 is not an *element* of A, or $5 \notin A$.

Definition 3.1.2. If X is a *finite* set, (it does not have an infinite number of elements), then it's **cardinality** (or **size**) is the number of elements it has. The **cardinality** of X is denoted by $|X|$. So for $A = \{2, 4, 6, 8\}$, $|A| = 4$.

Definition 3.1.3. The **empty set** is the set $\{\}$ that contains no elements. The empty set is represented as $\emptyset$, or ϕ. *Note:* $|\emptyset| = 0$

Caution: $\emptyset \neq \{\emptyset\}$. This is because the empty set, $\emptyset$ contains *nothing*, and $\{\emptyset\}$ contains one thing; the empty set, $\emptyset$.

Let $F = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$. This set contains three things:

(i) The empty set,
(ii) A set containing the empty set,

(iii) A set containing the set containing the empty set.

Thus, $|F| = 3$.

Definition 3.1.4. The **set-builder notation** is used to describe sets and their properties between braces. In general, a set X written with set-builder notation has the syntax

$$X = \{expression : rule\},$$

where the elements of X are understood to be all values of "expression" that are specified by the enclosed "rule."

Example: Consider the infinite set of integers $E = \{-3, -2, -1, 0, 1, 2, 3, ...\}$. In set-builder notation this set is written as

$$E = \{2n : n \in \mathbb{Z}\}.$$

We read the first brace as *"the set of all things of form,"* and the colon *"such that."* So the expression $E = \{2n : n \in \mathbb{Z}\}$ reads *E equals the set of all things of form* $2n$*, such that* n *is an element of* $\mathbb{Z}$*.*

3.2 Set Operations

3.2.1 The Cartesian Product

Given two sets A and B, it is possible to "multiply" them to produce a new set, denoted as $A \times B$. This operation is called the *Cartesian product*, or *cross-product*.

Definition 3.2.1. An **ordered pair** is a list (x,y) of two elements x and y, enclosed in parentheses and separated by a comma. Any list of two things enclosed by parentheses is an ordered pair.

For ordered pairs, (as the name implies) order matters. Thus, $(4, 2) \neq (2, 4)$.

Definition 3.2.2. The **Cartesian product** of two sets A and B is another set, denoted as $A \times B$ and defined as $A \times B = \{(a, b) : a \in A, b \in B\}$

So $A \times B$ is a set of ordered pairs of elements from A and B.

Example 1: Let $A = \{k, l, m\}$ and $B = \{q, r\}$, then

$$A \times B = \{(k, q), (k, r), (l, q), (l, r), (m, q), (m, r)\}.$$

Example 2: Let $A = \{0, 1\}$ and $B = \{2, 1\}$, then

$$\{0, 1\} \times \{2, 1\} = \{(0, 2), (0, 1), (1, 2), (1, 1)\}.$$

Note on the cardinality of Cartesian products: If A and B are finite sets, then

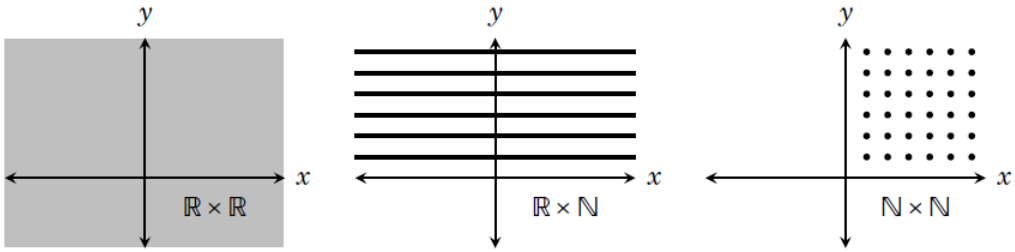
$$|A \times B| = |A| * |B|$$

Examples of Cartesian products:

The set $\mathbb{R} \times \mathbb{R} = \{(x, y) : x, y \in \mathbb{R}\}$ is the set of points on a Cartesian plane, as drawn in **Figure (a)** below.

The set $\mathbb{R} \times \mathbb{N} = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{N}\}$ is the set of all the points on the plane whose second coordinate is a natural number. (**Figure (b)**).

The set $\mathbb{N} \times \mathbb{N} = \{(x, y) : x, y \in \mathbb{N}\}$ is the set of all points on the plane whose coordinates are both natural numbers. (**Figure (c)**).



(a) (b) (c)

Cartesian products are also defined *beyond* ordered pairs. An **ordered triple** is a list (x, y, z). For example, the Cartesian product of the three sets $\mathbb{R}, \mathbb{N}$ and $\mathbb{Z}$ is $\mathbb{R} \times \mathbb{N} \times \mathbb{Z} = \{(x, y, z) : x \in \mathbb{R}, y \in \mathbb{N}, z \in \mathbb{Z}\}$. ***n*-tuples** can extend beyond ordered triples. In general,

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, ..., x_n) : x_1 \in A_i \text{ for each } i = 1, 2, ..., n\}.$$

Theorem 3.2.1. Some relationships between the products of sets and other set operations:

$A \times (B \cup C) = (A \times B) \cup (A \times C)$.
$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
$A \times \emptyset = \emptyset$.
$A \times B \neq B \times A$

Definition 3.2.3. For any set A and positive integer n, the **Cartesian power** A^n is

$$A^n = A \times A \times \cdots \times A = \{(x_1, x_2, ..., x_n) : x_1, x_2, ..., x_n \in A\}.$$

$\mathbb{R}^2$ is the familiar x, y Cartesian plane, $\mathbb{R}^3$ is the three-dimensional space. Referring back to the image of Cartesian products, we can see that if $\mathbb{R}^2$ is the plane, then $\mathbb{Z}^2$ is the is a grid of points on the plane. Likewise, as $\mathbb{R}^3$ is three-dimensional space, $\mathbb{Z}^3$ is a grid of points in space.

3.2.2 Subsets

Definition 3.2.4. Suppose A and B are sets. If every element of A is also an element of B, then we say A is a **subset** of B, and denote this as $A \subseteq B$. We write $A \not\subseteq B$ if A is *not* a

subset of B. Thus $A \not\subseteq B$ means there is at least one element of A that is *not* an element of B.

Note: If B is *ANY* set, then $\emptyset \subseteq B$. Therefore, the empty set is a subset of all sets, that is, $\emptyset \subseteq B$, for any set B.

In addition, the set B itself will also always be a subset of itself.

Theorem 3.2.2. If a *finite* set has n elements, then it has 2^n subsets. So, if $|B| = n$, then B has 2^n subsets.

Example: Let $B = \{1, 2, \{1, 3\}\}$. B has three elements: 1, 2, and $\{1, 3\}$. So $|B| = 3$, therefore $n = 3$, so B will have 2^3 subsets:

$$\{\}, \{1\}, \{2\}, \{\{1, 3\}\}, \{1, 2\}, \{1, \{1, 3\}\}, \{2, \{1, 3\}\}, \{1, 2, \{1, 3\}\}.$$

Subsets generally arise naturally. Consider the unit circle $C = \{(x, y) \in \mathbb{R}^2 : x^2+y^2 = 1\}$. This is a subset $C \subseteq \mathbb{R}^2$. Likeways the graph of a function $y = f(x)$ is a set of points $G = \{(x, f(x)) : x \in \mathbb{R}$, and $G \subseteq \mathbb{R}$.

Mathematics is filled with instances where it will be important to regard one set as a subset of another.

3.2.3 Power Sets

Given a set, you can form a new set with the *power set* operation.

Definition 3.2.5. If A is a set, the **power set** of A is *another set*, denoted as $\mathcal{P}(A)$ and defined to be all the subsets of A. In set-builder notation, $\mathcal{P}(A) = \{X : X \subseteq A\}$.

Note: if A is a finite set, then $|\mathcal{P}(A)| = 2^{|A|}$.

3.2.4 The Union, Intersection, and Difference of Sets

Definition 3.2.6. Suppose A and B are sets.

The **union** of A and B is the set	$A \cup B = \{x : x \in A \text{ or } x \in B\}$.
The **intersection** of A and B is the set	$A \cap B = \{x : x \in A \text{ and } x \in B\}$.
The **difference** of A and B is the set	$A - B = \{x : x \in A \text{ and } x \notin B\}$.

Definition 3.2.7. Sets A and B are **disjoint** if and only if $A \cap B = \emptyset$. This implies that they share *no common* elements.

Theorem 3.2.3. For all sets A, B, and C,

Statement	Reasoning
$A \subseteq B \cup B$	$A \cup B$ is inclusive, thus includes all elements in A *or* in B, so A is naturally a subset of the union.
$A \cap B \subseteq A$	By definition, the set $A \cap B$, implies every element is in *both* A and B. Since every element will be in A, $A \cap B$ will be a subset of A.
$A \cap \emptyset = \emptyset$	There are no elements in the empty set. There can be no elements in A that will also be in $\emptyset$, yielding only the empty set.
$A \cup \emptyset = A$	Since $A \cup \emptyset$ includes all elements in A *or* $\emptyset$, and the empty set contains no elements, this union can only produce all the elements that are in A.
$A \cap A = A$	If the intersection of the same sets contains elements in the same set, we *still only* have those elements in that set.
$A \cup A = A$	If the union of the same sets contains elements in the same set, we *still only* have those elements in that set.
$A - \emptyset = A$	Since the empty set contains nothing, you are subtracting nothing from A, therefore yielding A.
$\emptyset - A = \emptyset$	Since the empty set has no elements (*nothing*), you cannot have less than no elements, so you still only have the empty set.

General Laws for Sets

$A \cup (B \cup C) = (A \cup B) \cup C$	Associative Laws.
$A \cap B = B \cap A$	Commutative Laws.
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive Laws.

Note: When we work with sets whose elements are sets, it is important to recognize the distinction between "is an element of" and "is a subset of."

3.2.5 Complement of a Set

The **universe** of discourse is a collection of objects understood from the context or specified at the outset of a discussion and all objects under consideration *must* belong to the universe.

Definition 3.2.8. Let U be the universe and $A \subseteq U$. The **complement** of A is the set $A^c = U - A$. The complement of A can also be displayed as $\overline{A}$.

Theorem 3.2.4. Let U be the universe, and let A and B be subsets of U. Then

$(A^c)^c$	$=$	A.	
$A \cup A^c$	$=$	U.	
$A \cap A^c$	$=$	$\emptyset$.	
$A - B$	$=$	$A \cap B^c$.	
$A \subseteq B$	iff	$B^c \subseteq A^c$.	
$A \cap B = \emptyset$	iff	$A \subseteq B^c$.	
$(A \cup B)^c$	$=$	$A^c \cap B^c$.	De Morgan's Laws.
$(A \cap B)^c$	$=$	$A^c \cup B^c$.	De Morgan's Laws.

3.2.6 Indexed Sets

A set of sets is called a **family** or **collection** of sets. We use script letters, $\mathscr{A}, \mathscr{B}, \mathscr{C}, ...$ to denote families of sets. For example,

$$\mathscr{A} = \{\{1, 2, 3\}, \{3, 4, 5\}, \{3, 6\}, \{2, 3, 6, 7, 9, 10\}\}$$

is a family consisting of four sets. Notice that $5 \in \{3,4,5\}$ and $\{3,4,5\} \in \mathscr{A}$; ***but*** $5 \notin \mathscr{A}$.

Definition 3.2.9. Let $\mathscr{A}$ be a family of sets. The **union over** $\mathscr{A}$ is

$$\bigcup_{A\in\mathscr{A}} A = \{x : x \in A \text{ for some } A \in \mathscr{A}\}.$$

For any object x, this is compatible to

$$x \in \bigcup_{A\in\mathscr{A}} A \text{ iff } (\exists A \in \mathscr{A})(x \in A).$$

To show that an object is in the union of a family, we must show the existence of at least one set in the family that contains the object.

Definition 3.2.10. Let $\mathscr{A}$ be a family of sets. The **intersection over** $\mathscr{A}$ is

$$\bigcap_{A\in\mathscr{A}} A = \{x : x \in A \text{ for every } A \in \mathscr{A}\}.$$

For any object x, this is compatible to

$$x \in \bigcap_{A\in\mathscr{A}} A \text{ iff } (\forall A \in \mathscr{A})(x \in A).$$

Theorem 3.2.5. For every set B in a family $\mathscr{A}$ of sets,

1. $\bigcap_{A\in\mathscr{A}} A \subseteq B$.
2. $B \subseteq \bigcup_{A\in\mathscr{A}} A$.
3. If a family $\mathscr{A}$ is nonempty, then $\bigcap_{A\in\mathscr{A}} A \subseteq \bigcup_{A\in\mathscr{A}} A$.

Definition 3.2.11. Let Δ be a nonempty set such that for each $\alpha \in \Delta$ there is a corresponding set A_α. The family $\{A_\alpha : \alpha \in \Delta\}$ is an **indexed family of sets.** The set Δ is called the **indexing set** and each $\alpha \in \Delta$ is an **index**.

$$\overbrace{\{A_\alpha : \underbrace{\alpha}_{\text{index}} \in \underbrace{\Delta}_{\text{indexing set}}\}}^{\text{indexed family of sets}}.$$

An indexing family may be *finite* or *infinite*, the number of elements in the member sets do not have to be the same, and different indices do not need to correspond to different sets in the family.

For a family $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$, the notations for unions and intersection are:

$$\bigcup_{\alpha\in\Delta} A = \bigcup_{A\in\mathscr{A}} A \text{ and } x \in \bigcup_{\alpha\in\Delta} A_\alpha \text{ iff } (\exists\alpha \in \Delta)(x \in A_\alpha).$$

$$\bigcap_{\alpha\in\Delta} A = \bigcap_{A\in\mathscr{A}} A \text{ and } x \in \bigcap_{\alpha\in\Delta} A_\alpha \text{ iff } (\forall\alpha \in \Delta)(x \in A_\alpha).$$

Theorem 3.2.6. Let $\mathscr{A} = \{A_\alpha : \alpha \in \Delta\}$ be an indexed collection of sets. Then

1. $\bigcap_{\alpha\in\Delta} A_\alpha \subseteq A_\beta$ for each $\beta \in \Delta$.
2. $A_\beta \subseteq \bigcup_{\alpha\in\Delta} A_\alpha$ for each $\beta \in \Delta$.
3. $\left(\bigcap_{\alpha\in\Delta} A_\alpha\right)^c = \bigcup_{\alpha\in\Delta} A_\alpha^c$ } De Morgan's Laws
4. $\left(\bigcup_{\alpha\in\Delta} A_\alpha\right)^c = \bigcap_{\alpha\in\Delta} A_\alpha^c$ } De Morgan's Laws

Definition 3.2.12. The indexed family $\mathscr{A} = \{A_\alpha \in \Delta\}$ of sets is **pairwise disjoint** if and only if for all α and β in Δ, either $A_\alpha = A_\beta$ or $A_\alpha \cap A_\beta = \emptyset$.

3.3 Proofs for Set Theory

3.3.1 Proving A is a subset of B

You can use a direct proof to show that A is a subset of B.

Method of Proof:
Let x be any object.
Suppose $x \in A$.
$\quad\vdots$
Thus $x \in B$.
Therefore $A \subseteq B$.

Example: Let $A = \{2, 3\}$ and $B = \{x\ \mathbb{R} : x^3 + 3x^2 - 4x - 12 = 0\}$. Prove that $A \subseteq B$.

Proof: (Broken down)

Suppose $x \in A$.	Direct Proof: Suppose ..., then ...
Then $x = 2$ or $x = -3$.	Check each element of A
For $x = 2$,	Verifying first element
$(2)^3 + 3(2^2) - 4(2) - 12 = 0$	
$\quad = 8 + 12 - 8 - 12 = 0.$	
For $x = -3$,	Verifying second element
$(-3)^3 + 3(-3)^2 - 4(-3) - 12 = 0$	
$\quad = 0.$	
In both cases, $x \in B$.	Proved every element in A is also in B.
Thus, $A \subseteq B$.	

Proof. Suppose $x \in A$. Then $x = 2$ or $x = -3$. For $x = 2$, $(2)^3 + 3(2^2) - 4(2) - 12 = 0$ $= 8+12-8-12 = 0$. For $x = -3$, $(-3)^3+3(-3)^2-4(-3)-12 = 0 = -27+27+12-12 = 0$. In both cases, $x \in B$. Thus, $A \subseteq B$. □

4 Counting

Methods of counting are normally used in order to construct probability assignments on finite sample spaces.

Theorem 4.0.1. The Fundamental Theorem of Counting
If a job consists of k seperate tasks, the ith of which of which can be done in n_i ways, $i = 1, \ldots, k$, then the entire jobs can be done in $n_1 \times n_2 \times \cdots \times n_k$ ways.

4.1 Types of Counting Problems

	REPEATS NOT ALLOWED	REPEATS ALLOWED
ORDER MATTERS	$n(n-1)\cdots(n-k+1)$ Permutation	n^k
ORDER DOESN'T MATTER	$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}$ Combination	Break into cases

Definition 4.1.1. The **factorial** of a positive integer $n \in \mathbb{N}$ is

$$n! = n(n-1)\cdots 2 \cdot 1.$$

Furthermore, we define $0! = 1$.

Let $A = \{a, b, c\}$. Then, the *permutations* of this set will be:

$$\begin{array}{ll} \{a,b,c\} & \{c,a,b\} \\ \{b,a,c\} & \{a,c,b\} \\ \{c,b,a\} & \{b,a,c\} \end{array}$$

The number of permutations possible will be equal to the factorial of cardinality A, $|A|!$.

Definition 4.1.2. A **list** is an ordered sequence of objects. A list is denoted by an opening parenthesis, followed by the objects, separated by commas, followed by a closing parenthesis. Ex: $A = (a, b, c, d)$, where a, b, c, d are entries (or elements) of the list.

In a list, all elements have a definite order and can have repeated entries for the elements they contain. For example,

$$(a, b, c, d) \neq (d, c, b, a).$$

Also, (a, a, b, c, c) is a perfectly acceptable list, in contrast to sets.

Two lists are equal if and only if they have the same elements in exactly the same positions. Thus,

$$(0, 0, 0, 0) \neq (0, 0, 0).$$

I'm defining a list to overcome technicalities/issues that may appear when working with repeating/ordered elements.

4.1.1 Repeats Not Allowed, Order Matters

When we say "*Order Matters*", we are saying that order *is* taken into consideration, implying that $(a, b) \neq (b, a)$. **Note:** We turn the set into a *list* here since the sequence is now an *ordered* pair of objects. Thus, we are looking for the number of *permutations of the list* that can be achieved within the allotted number of options.

From the *Fundamental Theorem of Counting*, the first number can be selected n ways, the second $n-1$ ways, the third $n-2$ ways, and so on, until we get to the kth selection, for which we have $n-k+1$ choices. If the order in which these selections matter, then the total number of possibilities will be

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

What we are doing here is defining the total number of permutations of n, and then dividing them by the difference between n and k, the number of tasks.

To achieve a faster method, let us show

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

So we have

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

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

$$= n(n-1)(n-2)\cdots(n-k+1).$$

Definition 4.1.3. A **k-permutation** of an n-element set is a non-repetitive length-k list made from k elements of the set. Informally we think of a k-permutation as an arrangement of k of the set's elements in a row. The number of k-permutations of an n-element is denoted

$$P(n, k) = n(n-1)(n-2)\cdots(n-k+1).$$

This equation simply implies that you take the factorial of n and cut it off once the number of times you multiplied it reaches k (the number of tasks).

This is used in the cases when you are taking *order* into account, i.e., **permutations.**

Let $A = \{a, b, c, d\}$. Let's say we wanted to know how many options we would have if we wanted to produce a *list* of cardinality 2. Then, we would have $n = |A|$, so $n = 4$, and $k = 2$, giving us

$$\underbrace{4}_{\text{1st Choice}} \times \underbrace{(4-2+1)}_{\text{2nd Choice}} = 12.$$

The permutations this would produce would be:

$$\begin{array}{lll} (a,b) & (a,d) & (c,d) \\ (b,a) & (d,a) & (d,c) \\ (a,c) & (b,d) & (b,c) \\ (c,a) & (d,b) & (c,b) \end{array}$$

4.1.2 Repeats Not Allowed, Order Doesn't Matter

When we say "*order doesn't matter*", what we mean is *order is not taken into consideration.* So $\{a,b\} = \{b,a\}$. So we are not looking for the number of *permutations* that can be achieved, but the number of **combinations** that can.

Definition 4.1.4. The numbers $\binom{n}{k}$, with $0 \leq k \leq n$, are called the **binomial coefficients**, read "*n choose k*," and defined by the formula

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

The *binomial coefficient* can also be interpreted as *the nnumber of combinations of k elements taken from a set of n, when order does not matter.*

An equivalent formula that can be used for binomial coefficients is:

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

Theorem 4.1.1. Binomial Theorem. For any integer $n > 0$, and for any real numbers x and y, with $(x,y) \neq (0,0) if n = 0$), we have that

$$(x+y)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^{n-k} y^k.$$

The *Binomial Theorem* above, along with *Pascal's Triangle* will be addressed later.

4.1.3 Repeats are Allowed, Order Matters

Suppose that repeats are allowed and order matters. If we are selecting elements from a set of cardinality n then we have n choices for the first selection, n choices for the second selection, and so on. Therefore, we have n choices *for all* k of our selections. Therefore, if order of selection matters and repeated selections are allowed, then the number of ways of choosing k objects from a collection of n is

$$\underbrace{n \cdot n \cdots n}_{k\text{-times}} = n^k.$$

This is valid even if k is larger than n, due to the fact that repeats are being allowed.

4.1.4 Repeated Selections are Allowed, Order Doesn't Matter

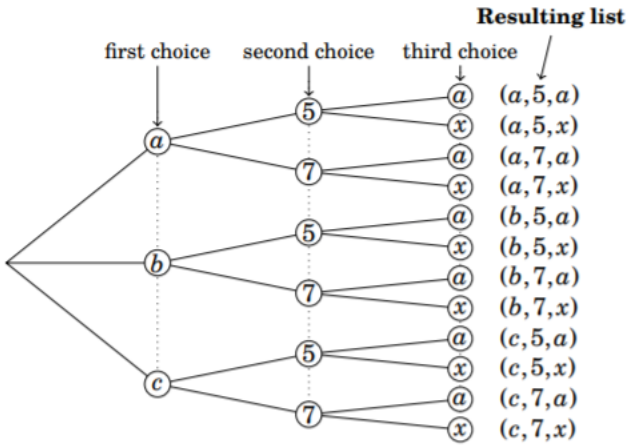
We will be breaking these up into cases. Each case will consist of some form of the cases stated above. Good luck.

4.2 The Multiplication Principle

Many practical problems involve counting the number of possible outcomes that satisfy some condition or property.

Suppose we make a list of length three having the property that the first entry must be an element of the set $\{a, b, c\}$, the second entry must be in $\{5, 7\}$, and the thrid tnry must be in $\{a, x\}$. How many lists are there all together?

The choices for the first entry are a, b, or c, and the start of the diagram branches out in three directions, one for each choice. Once this choice is made there are two choices (5 or 7) for the second entry, which yields two more branches for each choice, from each of the three choices from the first entry. This pattern continues for the choice for the third entry, which is either a or x. So in the diagram, there are $3 \cdot 2 \cdot 2 = 12$ paths from left to right.



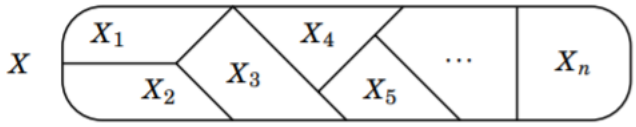
Definition 4.2.1. Multiplication Principle. Suppose in making a list of length n there are a_1 possible choices for the first entry, a_2 possible choices for the second entry, a_3 possible choices for the third entry, and so on. Then the total number of different lists that can be made this way is the product $a_1 \cdot a_2 \cdot a_3 \cdots a_n$.

4.3 The Addition and Subtraction Principles

4.3.1 The Addition Principle

The *addition principle* simply states that if a set can be broken into pieces, then the size of the set is the sum of the sizes of the pieces. *Note:* See pairwise disjoint/partition properties.

Definition 4.3.1. (Addition Principle) Suppose a finite set X can be decomposed as a union $X = X_1 \cup X_2 \cup \cdots \cup X_n$, where $X_i \cap X_j = \emptyset$ wherever $i \neq j$. Then $|X| = |X_1| + |X_2| + \cdots + |X_n|$. The figure below gives an idea of what this may look like.



We use the addition principle when we need to count the things in some set X. If we can find a way to break X up as $X = X_1 \cup X_2 \cup \cdots X_n$, where each X_i is easier to count than X, then the addition principle gives an answer of $|X| = |X_1| + |X_2| + |X_3| + \cdots |X_n|$.

but for this to work, the intersection of *any* two pieces X_i must be $\emptyset$, otherwise you run into the issue of double-counting. (This will be detailed later in the *Inclusion-Exclusion Principle.*)

4.3.2 The Subtraction Principle

Definition 4.3.2. If X is a subset of a finite set U, then $|X^c| = |U| - |X|$. In other words, if $X \subseteq U$, then $|U - X| = |U| - |X|$.

The subtraction principle is used in situations where it is easier to count the things in some set U that we wish to *exclude* from consideration than it is to count those things that are included.

4.4 The Inclusion-Exclusion Principle

Suppose we have two finite sets, A and B, and we are interested in determining the number of elements in their union $A \cup B$. From the *addition principle*, If A and B are disjoint then $A \cap B = \emptyset$, and we have that

$$|A \dot{\cup} B| = |A| + |B|.$$

This extends to finite unions of *pairwise disjoint* sets. If $A_1, A_2, \ldots A_n$ are finite sets *which are pairwise disjoint*, then

$$\left| \dot{\bigcup_{1 \le i \le n}} A_i \right| = |A_1| + |A_2| + \cdots + |A_n|.$$

What happens if A and B are not disjoint? Well, then there exists elements that are in A and in B, which then will be counted *twice*, resulting in an incorrect sum, since there are elements that are counted twice. So *Note!* $|A \cup B| \neq |A| + |B|$ if A and B are *NOT* disjoint.

To account for this, we subtract $|A \cup B|$ to obtain the formula

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Now suppose that we have three finite sets, A_1, A_2, and A_3, and wish to obtain the number of elements in $A_1 \cup A_2 \cup A_3$. Then, we will use

$$\begin{aligned} &|A_1| + |A_2| + |A_3| \\ &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

How this logic works:

$\|A_1\| + \|A_2\| + \|A_3\|$	
$= \|A_1\| + \|A_2\| + \|A_3\|$	Adds the initial elements of the sets together
$-\|A_1 \cap A_2\| - \|A_1 \cap A_3\| - \|A_2 \cap A_3\|$	Subtracts elements in intersection of individual sets
$+\|A_1 \cap A_2 \cap A_3\|.$	Adds back elements of the *family's* intersection

Theorem 4.4.1. (Inclusion-Exclusion Principle) If $A_1, A_2, \ldots, A_n$ are finite sets, then

$$\begin{aligned}\left|\bigcup_{1\le i\le n} A_i\right| &= \sum_{1\le i\le n} |A_i| \\ &- \sum_{1\le i\le j\le n} |A_i \cap A_j| \\ &+ \sum_{1\le i\le j\le n} |A_i \cap A_j \cap A_k| \\ &- \cdots \\ &+ (-1)^{n-1}|A_1 \cap A_2 \cap \cdots \cap A_n|.\end{aligned}$$

4.5 Countable vs. Uncountable

Sample spaces can be either *countable* or *uncountable*; if the elements can be put into 1-1 correspondence with a subset of the integers ($\mathbb{Z}$), the sample space is countable. Also, if the sample space contains only a finite number of elements, it is countable.

This implies that sample spaces which consist of real numbers ($\mathbb{R}$) are not countable, since the real-number system cannot be put into 1-1 correspondence with the integers.

5 Mathematical Induction

5.1 Principle of Mathematical Induction

5.2 Principle of Complete Induction

6 Relations

Definition 6.0.1. A **relation** on a set A is a subset $R \subseteq A \times A$. The statement claiming that elements are part of a relation is shown as $(x, y) \in R$ and is abbreviated $x\ R\ y$.
Note: The relation is another set, (in fact, it's a subset of the two sets it is related to).

Since relations from set A to set B are subsets of $A \times B$, the union and intersection are also relations from A to B.

Definition 6.0.2. The **domain** of the relation R from A to B is the set
$\text{Dom}(R) = \{x \in A : \text{there exists } y \in B \text{ such that } x\ R\ y\}$.

The **range** of the relation R is the set
$\text{Rng}\ (R) = \{y \in B : \text{there exists } x \in A \text{ such that } x\ R\ y\}$.

Therefore by definition, the $\text{Dom}(R) \subseteq A$ and the $\text{Rng}\ (R) \subseteq B$.

Definition 6.0.3. For any set A, the relation $I_A = \{(x, x) : x \in A\}$ is called the **identity relation on** A.

Definition 6.0.4. If R is a relation from A to B, then the **inverse** of R is the relation

$$R^{-1} = \{(y, x) : (x, y) \in R\}.$$

Theorem 6.0.1. Let R be a relation from A to B.

$$\text{Dom}(R^{-1}) = \text{Rng}\ (R)$$
$$\text{Rng}(R^{-1}) = \text{Dom}(R)$$

Definition 6.0.5. Let R be a relation from A to B, and let S be a relation from B to C. The **composite** of R and S is

$$S \circ R = \{(a, c) : \exists b \in B \text{ s.t. } (a, b) \in R \text{ and } (b, c) \in S\}.$$

7 Functions

Appendices

7.A The Division Algorithm and Bézout's Identity

Axiom *The Well-Ordering Principle (WOP)*: Every non-empty subset of $\mathbb{N}$ has a smallest element.

Theorem 7.A.1. The Division Algorithm. Given two integers a and b with $b > 0$, there exists unique integers q and r such that

$$a = qb + r, \ 0 \leq r < b$$

where a is the divisor, q is the quotient, and r is the remainder.

Definition 7.A.1. Let a, b, c and d be nonzero integers.

We say c is a **common divisor** iff $c|a$ and $c|b$

We say d is the **greatest common divisor (gcd)** of a and b and write $d = \gcd(a, b)$ iff

a. d is a common divisor of a and b.

b. every common divisor c of a and b is less than or equal to d.

Note: The gcd is always a positive number.

Definition 7.A.2. An integer of the form $ax + by$, for integers x and y is called a **linear combination** of a and b.

Theorem 7.A.2. Bézout's Identity. Let a and b be nonzero integers. The $\gcd(a, b)$ is the *smallest* positive *linear combination* of a and b.

We use Bézout's Identity to derive the following results regarding divisibility.

Theorem 7.A.3. Euclid's Lemma If $a|bc$ with $\gcd(a, b) = 1$, then $a|c$. Colloquially: Let p be a prime number, and let a and b be integers, if $p|ab$ then $p|a$ or $p|b$.

Proof. Since $\gcd(a, b) = 1$ there exists integers m and n such that $am + bn + 1$. Multiplying c on both sides, we get $c = acm + bcn$. Since $a|bc$ and $a|acm$, we get $a|c$. □

Theorem 7.A.4. If $a|c$ and $b|c$ with $\gcd(a, b) = 1$, then $ab|c$.

Proof. Since $\gcd(a, b) = 1$, there exist integers m and n such that $am + bn = 1$. Multiplying c on both sides, we get $c = c(am + bn) = acm + bcn$. Now since $b|c$ so $ab|ac$ and similarly $ab|bc$, so $ab|c$. □

7.B Congruence