Math 277
Discrete Structures Notes

Carter Clifton

Fall 2024

Contents

Chapter 1

Fundamental Principles of Counting

Introduction

The first question that should come to your mind here is, "What do you mean by counting?" Everyone learns the basics of counting, or enumeration in elementary school, but the techniques of counting have been developed to deal with much harder problems. One reason is that it is a difficult concept to grasp since formulas will not be given to solve each problem. Instead you must analyse each problem to determine which formula(s) apply.

Example 1.0.1

How many even numbers are there between 52 and 88 (inclusive)?

$$88 - 52 = 36$$

$$36/2 = 18$$

$$18 + 1 = 19$$

There are 19 even numbers between 52 and 88.

Theorem 1.0.2

If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

Example 1.0.3

What is the 13th element of the array $A[24], A[25], A[26], \ldots, A[104]$?

1.1 The Rules of Sum and Product

The study of combinatorial mathematics begins with two basic principles of counting : the rules of sum and product. Enumeration, in complicated problems is often solved by breaking down problems into simpler pieces, each of which can be solved using these basic principles.

Definition 1.1.1 : The Rule of Sum

If a first task can be performed in m ways, while a second task can be performed in n ways, and the two tasks cannot be performed simultaneously, then performing either task can be accompilshed in any one of $m + n$ ways.
The signal that one should use the rule of sum is the word **or**.

Example 1.1.2

It is Friday night and you have been invited to three parties. You could also go to a movie. There are five movies playing at the Antigonish theatre. Assuming you go to one party or one movie (but not both), in how many ways can you spend your evening?

$$3 + 5 = 8$$

There are 8 ways you could spend your evening.

Example 1.1.3

In how many ways can a person get a total of four when a black die and a blue die are rolled?

$$\left[\begin{array}{c|ccc} \textit{Black} & 1 & 2 & 3 \\ \textit{Blue} & 3 & 2 & 1 \end{array}\right]$$

$$1 + 1 + 1 = 3$$

There are three ways a person could get a total of four.

Definition 1.1.4 : The Rule of Product

If a procedure can be broken down into a first and a second stage, and if there are m ways to perform the first stage and for each of these, there are n ways to perform the second stage, then the total procedure can be carried out, in the designated order, in $m * n$ ways.
This rule can be extended to any finite number of stages. It is sometimes referred to as the *principle of choice*.
The keyword **and** is a signal to use the Rule of Product.

Example 1.1.5

Back to Friday night's choices! Assuming now you would like to go to a movie first (5 choices) and then to a party afterwards (3 choices), in how many ways can you now spend the evening?

$$5 * 3 = 15$$

There are 15 ways you could spend the evening.

Example 1.1.6

(a) Suppose a computer password consists of 5 letters from the English (Latin) alphabet. Repetition of letters is allowed and case is not important. How many different passwords are possible?

$$26 * 26 * 26 * 26 * 26 = 26^5$$

There are 26^5 different possible passwords.
(b) Suppose no repetition of letters is allowed. How many different passwords are now possible?

$$26 * 25 * 24 * 23 * 22 = \frac{26!}{21!}$$

There are $\frac{26!}{21!}$ different possible passwords.

The Dreaded Over Counting

The Rule of Product is not always easy to apply. In fact, in some situations it will lead you to an incorrect solution if you are not careful!

Example 1.1.7

(a) Consider the following problem. Three officers, a president, a treasurer, and a secretary, are to be chosen from among four people: Ann, Babak, Chin and Dopey. In how many ways can the officers be chosen?

$$4 * 3 * 2 = 24$$

There are 24 ways the officers can be chosen.
(b) Now suppose that Ann cannot be the president and either Chin or Dopey must be the secretary. In how many ways can the officers now be chosen?

$$2 * 2 * 2$$

There are 8 ways the officers can now be chosen.

Example 1.1.8

(a) Suppose a blue die and a black die are rolled. How many distinct outcomes are possible?

$$6 * 6 = 36$$

There are 36 distinct possible outcomes.
(b) Now suppose the two dice are identical looking. How many different outcomes are possible?
One dice must be roll a value lower or equal to the other.

Lower Dice	Higher Dice
1	1, 2, 3, 4, 5 or 6
2	2, 3, 4, 5, or 6
3	3, 4, 5, or 6
4	4, 5, or 6
5	5 or 6
6	6

$$6 + 5 + 4 + 3 + 2 + 1 = 21$$

There are 21 different outcomes possible.

Example 1.1.9

How many numbers between 10000 and 99999 contain at least one 1?

$$99999 - 10000 + 1 = 90000$$

$$90000 - (8 * 9 * 9 * 9 * 9) = 37512$$

37512 numbers contain at least one 1.

1.2 Permutations

Definition 1.2.1 : Factorials

For any integer $n \geq 0$, "n factorial", denoted $n!$, is defined by:

$$0! = 1$$

$$n! = n * (n - 1)!$$

Example 1.2.2

$$3! = 3 * 2 * 1 = 6$$

$$6! = 6 * 5 * 4 * 3 * 2 * 1 = 720$$

Factorial expressions grow quickly! For example, 10! = 3628800 represents the amount of seconds in six weeks; whereas 13! = 6227020800 exceeds the number of seconds in a century. Check it out! The earth is approximately 4.5 billion years old. What number is the smallest value of n such that $n!$ exceeds the age of the earth in seconds?

$$4.5 \text{ billion} * 365 * 24 * 60 * 60 \approx 20!$$

Definition 1.2.3 : Permutations

Given a collection of n distinct objects (with no repetition allowed), any (linear) arrangement of these objects is called a permutation of the collection.

Example 1.2.4

Rupert, my cat, has three friends over to a party. How many ways can they be permuted?

$$4 * 3 * 2 * 1 = 4!$$

There are 4! ways to permute the cats.

Example 1.2.5

Given 6 people, (a) in how many ways can they be arranged in a line?

$$6 * 5 * 4 * 3 * 2 * 1 = 6!$$

There are 6! ways to arrange them in a line.
(b) in how many ways can they be arranged with person #6 and person #5 beside each other?
"Glue" the two people together

$$2 * 1 = 2!$$

There are 2! ways for person #6 and person #5 to be arranged.

$$5 * 4 * 3 * 2 * 1 = 5!$$

There are 5! ways for 4 people, and the group of person #6 and person #5 to be arranged.
So, there are $5! * 2!$ ways the people can be arranged where person #6 and person #5 are beside each other.

Example 1.2.6

In how many ways can 3 people from a group of 8 people be arranged in a line?

$$8 * 7 * 6 = \frac{8!}{5!}$$

There are $\frac{8!}{5!}$ ways that 3 of the 8 people could be arranged.

Theorem 1.2.7

Given n disinct objects and an integer r, $1 \leq r \leq n$, then by the rule of product, the number of permutations of size r for the n objects is given by:

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

Definition 1.2.8 : R-Permutations

We call a permutation of size r an r-permutation. The number of r-permutations of a collection of n objects is denoted by the symbol $P(n, r)$.

$$P(n, r) = \frac{n!}{(n-r)!}$$

Special Cases:

- $P(n, 0) = 1$ (# of ways to make an empty selection)
- $P(n, n) = n!$ (# of ways to select all objects)

Example 1.2.9

(a) The number of permutations of the letters in the word OILERS is

$$6 * 5 * 4 * 3 * 2 * 1 = 6!$$

(b) If only four of the letters are used, then the number of 4-permutations is

$$\frac{6!}{(6-4)!} = \frac{6!}{2!}$$

(c) If repetition is allowed, the number of linear arrangements of five letters is

$$6 * 6 * 6 * 6 * 6 = 6^5$$

Example 1.2.10

In how many ways can the letters of CARIBOO be arranged?
Let's begin by assuming the two O's are distinguishable. Notice the permutations can be grouped ito pairs where each pair has the O's in the same places (but in the opposite order).
There are $2 * 1 = 2!$ ways the O's can be arranged, so the total number of groups is

$$\frac{7!}{2!}$$

Example 1.2.11

In how many ways can the letters of REPLETE be arranged?
There are 3 repeated E's that can be arranged in $3 * 2 * 1 = 3!$ ways.

$$\frac{7!}{3!}$$

Theorem 1.2.12

Given n objects with n_1 of the first type, n_2 of a second type, ..., and n_k of a k^{th} type, where $n_1 + n_2 + \cdots + n_k = n$, there are

$$\frac{n!}{n_1! * n_2! * \cdots * n_k!}$$

(linear) arrangements of the given n objects.

Example 1.2.13

(a) In how many ways can the letters of the word MISSISSIPPI be arranged?
There is 1 M, 4 I's, 4 S's, and 2 P's.

$$\frac{11!}{4! * 4! * 2!}$$

(b) How many arrangements are there in which all four S's are together?
"Glue" the S's together, $\frac{4!}{4!}$
Now you have 1 M, 4 I's, 1 SSSS, and 2 P's.

$$\frac{8!}{4! * 2!}$$

Example 1.2.14

(a) In how many ways can eight people be arranged in a circle if arrangements are considered the same when one can be obtained from the other by a rotation?
Solution 1: Since a circle has no beginning and no end, fix one person on the circle and place all the remaining people relative to this person.

$$7!$$

Solution 2: Arrange the people around the circle by wrapping a linear arrangement around the circle. Next group the arrangements together in collections so that all arrangements in each collection can be obtained from each other by rotation, i.e., we consider all arrangements in one group as equivalent.

$$\frac{8!}{8} = 7!$$

(b) Suppose two of the eight people refuse to sit next to each other around the circle. How many circular arrangements are now possible.
"Glue" the two people together. There are $6! * 2!$ ways to arrange the 6 people and the pair of 2. now, take away that away from the total number of possibilities, 7!, and you get

$$7! - 6! * 2!$$

1.3 Combinations : The Binomial Theorem

Definition 1.3.1 : Combinations

Given nonnegative integers n and r with $0 \leq r \leq n$, an unordered selection of r elements taken from n elements is called a combination. The symbols $C(n, r)$ or $\binom{n}{r}$, read "n choose r", are used interchangeably to represent the number of r-combinations (subsets of size r) taken from a set of n elements.

Example 1.3.2

Catan, Miles, and Pandora are playing games and running up and down the floors of my neighbour's house.

r-combinations	Cats on the main floor	number
0-combinations	-	1
1-combinations	C, M, P	3
2-combinations	CM, MP, PC	3
3-combinations	CMP	1

Example 1.3.3

How do we compute $\binom{n}{r}$ without listing all the possibilities? As before, let's begin with r-permutations and define two r-permutations to be the same if one is a reordering of the other.
$P(n, r) = \frac{n!}{(n-r)!}$ is the same as choosing r objects from n and lining them up. There are $r!$ ways to line up the r objects chosen. So, $P(n, r) = \binom{n}{r} * r!$.

Theorem 1.3.4

Given integers n and r with $0 \leq r \leq n$,

$$C(n,r) = \binom{n}{r} = \frac{n!}{r! * (n-r)!}$$

Example 1.3.5

(a) How many 5 person committees can be chosen from a group of 13 people?

$$\binom{13}{5}$$

(b) How many if one member of the group will not serve on any committee?

$$\binom{12}{5}$$

(c) How many if there are 2 people who insist on being on any commitees together?

$$\binom{11}{3} + \binom{11}{5}$$

(d) How many if 2 people do not get along and must not sit on any committee together?

$$\binom{13}{5} - \binom{11}{3} \text{ or } \binom{11}{4} + \binom{11}{4} + \binom{11}{5}$$

Example 1.3.6

How many teams can be formed from 7 women and 4 men if
(a) the team consists of 3 women and 2 men?

$$\binom{7}{3} * \binom{4}{2}$$

(b) the team consists of an equal number of women and men?

$$\binom{7}{4} * \binom{4}{4} + \binom{7}{3} * \binom{4}{3} + \binom{7}{2} * \binom{4}{2} + \binom{7}{1} * \binom{4}{1} + \binom{7}{0} * \binom{4}{0}$$

(c) the team consists of 4 people, at least two of which are women?

$$\binom{7}{2} * \binom{4}{2} + \binom{7}{3} * \binom{4}{1} + \binom{7}{4} * \binom{4}{0}$$

Example 1.3.7

(a) In how many ways can the letters of MISSISSIPPI be arranged?

$$\frac{11!}{4! * 4! * 2!}$$

(b) How many of these arrangements have no adjacent S's?
Arrange all the non-S letters.

$$\frac{7!}{4! * 2!}$$

These 7 letters have 8 gaps (between the letters + front + back), so the S's have $\binom{8}{4}$ spaces to go.

$$\frac{7!}{4! * 2!} * \binom{8}{4}$$

Example 1.3.8

(a) How many 5 card hands can be dealt from a standard 52 card deck?

$$\binom{52}{5}$$

(b) How many of these hands contain exactly one club?

$$\binom{13}{1}+\binom{39}{4}$$

(c) How many of these hands contain at least one club?

$$\binom{52}{5}-\binom{39}{5}$$

or consider each case individually

$$\binom{13}{1}\binom{39}{4}+\binom{13}{2}\binom{39}{3}+\binom{13}{3}\binom{39}{2}+\binom{13}{4}\binom{39}{1}+\binom{13}{5}\binom{39}{0}$$

Theorem 1.3.9

For any integer n and r with $0 \leq r \leq n$:

$$\binom{n}{r}=\binom{n}{n-r}$$

Whenever a selection of r objects is made from n objects, the process leaves behind $n-r$ objects. The followiung theorem is an easy consequence of this observation.

The Algebra of Combinatorics : Pascal's Triangle

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

The binominal coefficients can be arranged in a triangle so that each entry is the sum of the two previous entries (or the entry is on the boundary and has value 1). Even though we attach Blaise Pascal's name to the Triangle and the following formula it was known in the Arabic and Chinese worlds long before Pascal. The triangle appears in the work of Yang Hui (ca. 1261 - 1275) and Chu Shih-Chieh (1280 - 1303). In fact, there are references to the triangle as early as 1100. The triangle was also known to the famous Persian mathematician (and poet) Omar Khayyam (1048 - 1131).

Theorem 1.3.10

Let n and r be integers with $1 \leq r \leq n$. Then,

$$\binom{n+1}{r}=\binom{n}{r}+\binom{n}{r-1}$$

This formula describes the pattern in the triangle (Pascal's Formula).

Proof 1 (Algebraic Approach)

$$\binom{n+1}{r}$$

$$\frac{(n+1)!}{r!(n+1-r)!}$$
$$\frac{(n+1)n!}{r!(n+1-r)!}$$
$$(n+1)\frac{n!}{r!(n+1-r)(n-r)!}$$
$$\frac{n+1}{n+1-r} * \frac{n!}{r!(n-r)!}$$
$$\vdots$$
$$\frac{n!}{r!(n-r)!} + \frac{n!}{(r-1)!(n-r+1)!}$$
$$\binom{n}{r} + \binom{n}{r+1}$$

Proof 2 (Combinatorical Approach)

1. Siena has $n+1$ pairs of shoes and needs to select r of them to take to the hotel with her. This can be done in $\binom{n+1}{r}$ = LHS ways.
2. RHS counts the same thing by identifying her favourite pari of shoes and either bring them or not. There are $\binom{n}{r}$ ways to select the shoes if she doesn't bring her favourites and there are $\binom{n}{r-1}$ ways to select the shoes to bring i she does bring her favourites. The RHS follows from the rule of sum.

Theorem 1.3.11

The Binomial Theorem : Suppose x and y are variables and n is a positive integer. Then

$$(x+y)^n$$
$$= \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \binom{n}{2}x^2y^{n-2} + \cdots + \binom{n}{n-1}x^{n-1}y^1 + \binom{n}{n}x^ny^0$$
$$= \sum_{i=0}^{n}\binom{n}{i}(x^i)(y^{n-i})$$

This proof of this theorem is accomplished by considering the terms in $(x+y)^n$. Each term consists of n letters. For example, if there are k x's, then there must be $n-k$ y's. Given k x's and $n-k$ y's, there are $\frac{n!}{k!(n-k)!} = \binom{n}{k}$ ways to arrange the letters.

Example 1.3.12

(a) What is $(a+b)^3$?

$$\binom{3}{0}a^3b^0 + \binom{3}{1}a^2b^1 + \binom{3}{2}a^1b^2 + \binom{3}{3}a^0b^3$$

(b) What is $(1-z)^6$?

$$\binom{6}{0}1^6(-z)^0 + \binom{6}{1}1^5(-z)^1 + \binom{6}{2}1^4(-z)^2 + \cdots + \binom{6}{5}1^1(-z)^5 + \binom{6}{6}1^0(-z)^6$$
$$= 1 - \binom{6}{1}z + \binom{6}{2}z^2 - \binom{6}{3}z^3 + \binom{6}{4}z^4 - \binom{6}{5}z^5 + \binom{6}{6}z^6$$

Example 1.3.13

(a) The coefficient of x^3y^5 in the expansion of $(x+y)^8$ is

$$\binom{8}{5} \text{ or } \binom{8}{3}$$

(b) The coefficient of a^3b^5 in the expansion of $(3a-2b)^8$ is

$$\binom{8}{5} * 3^3 * (-2)^5 \text{ or } \binom{8}{3} * 3^3 * (-2)^5$$

Corollary 1.3.14

For any integer $n > 0$,

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$$

and

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots (-1)^n \binom{n}{n} = 0$$

The first statement follows from the Binomial Theorem with $x = y = 1$ and the second follows from the Binomial Theorem with $x = -1$, $y = 1$.

1.4 Combinations with Repetition : Distributions

We have already studied the number of ways to choose r objects, without replacement, from a set of size n where the order of the selections does not matter - the result is $\binom{n}{r}$. Now consider the problem of choosing r objects from n, again the order of selections does not matter, but each object may be selected more than once.

Example 1.4.1

How many unordered selections of 4 objects from the set $\{a, b, c\}$ are there if repetition is allowed?
Solution 1: Let's try our previous trick with grouping equivalent objects. That is, let's count the number of selections of 4 objects *with replacement* and group together those selections that are the same when order is removed.

aaaa	*aaab*	*aaac*
aabb	*aabc*	*aacc*
abbb	*abbc*	*abcc*
accc	*bbbb*	*bbbc*
bbcc	*bccc*	*cccc*

Solution 2: Let's agree on a standard way to list a selection. That is, by using alphabetical order, a selection of four objects has a standard, or what mathematicians call a *canonical*, representation. We can now simply list all four letter selections.

aaaa	*aaab*	*aaac*	*aabb*	*aabc*
aacc	*abbb*	*abbc*	*abcc*	*accc*
bbbb	*bbbc*	*bbcc*	*bccc*	*cccc*

That answer to the question is there are 15 unordered selections with replacement. How can we solve this problem without listing all possibilities? We develop a general formula for counting the number of such selections. The crux of the development is to associate each selection above with a binary string that contains exactly two zeros. Since the order in which the letters above are selected does not matter, we can always order the letters so that all the a's come first, the b's come second, and the c's come third, i.e., use

the canonical representation. For each selection construct a binary sequence. For example, the selection *aabc* corresponds to the sequence 110101. The 0's act as separators between different types of objects, the 1's tell us how many of each object there is. Together:

a	a		b		c
1	1	0	1	0	1

Hence, we can count the numebr of selections if, and only if, we can count the number of binary strings of length six that contain exactly four 1's, and two 0's. This is equivalent to simply choosing four locations out of the six to put the 1's in, i.e., there are $\binom{6}{4}$ such strings. Notice there is an easy confirmation here that $\binom{6}{4} = \binom{6}{2}$. **Note:** Some authors use "x" and "|" instead of "1" and "0".

Theorem 1.4.2

The number of unordered selections, with repetition, of r objects from a set of n objects is given by:

$$\frac{\begin{matrix} r \text{ 1's} \\ n-1 \text{ 0's} \end{matrix}}{n+r-1 \text{ total}} \rightarrow \frac{(n+r-1)!}{r!(n-1)!} = \binom{n+r-1}{r}$$

We can now summarize the four types of selections of r objects from n objects:

	With Replacement	Without Replacement
Ordered Selections	n^r	$P(n,r)$
Unordered Selections	$\binom{n+r-1}{r}$	$\binom{n}{r}$

Example 1.4.3

"Terri's Twenty-Two Types" boasts 22 different flavours of ice cream. Terri sells a "banana-split-light" that has three scoops of ice cream but no toppings. Assuming that the order of the scoops does not matter (e.g., "chocolate, strawberry, vanilla" is the same as "vanilla, chocolate, strawberry")
(a) How many different banana-split-lights exist?

3 1's, 21 O's (switches) $\rightarrow$ 24 Total

$$\frac{21!}{3!21!} = \binom{24}{3} = \binom{24}{21}$$

(b) How many have repeated flavours?

All - No repeated flavour

$$\binom{24}{3} - \binom{22}{3}$$

Example 1.4.4

Suppose that Terri decides to run a special sale where, for a limited time only, one can get sprinkles on the middle scoop in the banana-split-light for no extra charge. So now, "chocolate, strawberry, vanilla" is equivalent to "vanilla, strawberry, chocolate" but it is not equivalent to "chocolate, vanilla, strawberry".
(a) How many different banana-split-light-with-middle-sprinkles are there?

$$\binom{23}{2} * 22$$

(b) How many have repeated flavours?

$$\binom{23}{2} * 22 - \binom{21}{2} * 22$$

Example 1.4.5

(a) How many solutions to the equation

$$x_1 + x_2 + x_3 + x_4 = 10, \text{ where } x_i \geq 0, \text{ for } 1 \leq i \leq 4$$

are there? Note that $x_1 = 2$, $x_2 = 2$, $x_3 = 2$, $x_4 = 4$ and $x_1 = 4$, $x_2 = 2$, $x_3 = 2$, $x_4 = 2$ are two different solutions. One way to approach this problem is to think of distributing ten identical balls into four distinct containers, one container for each x_i.

$$\text{10 1's, 3 0's, 13 total } \rightarrow \binom{13}{3}$$

(b) How many solutions to the equation

$$x_1 + x_2 + x_3 + x_4 = 10, \text{ where } x_i > 0, \text{ for } 1 \leq i \leq 4$$

are there?

$$x_i > 0 \rightarrow x_i - 1 \geq 0 \text{ for } 1 \leq i \leq 4$$

$$(x_1 - 1) + (x_2 - 1) + (x_3 - 1) + (x_4 - 1) = 10 - (1 * 4) = 6$$

$$\text{6 1's, 3 0's, 9 total} \rightarrow \binom{9}{3}$$

Example 1.4.6

How many solutions to the inequality

$$x_1 + x_2 + x_3 + x_4 < 10, \text{ where } x_i \geq 0, \text{ for } 1 \leq i \leq 4$$

are there?

$$x_1 + x_2 + x_3 + x_4 \leq 9$$

$$x_1 + x_2 + x_3 + x_4 = 9 - x_s \text{ (Slack variable)}$$

$$x_1 + x_2 + x_3 + x_4 + x_s = 9 \text{ where } x_i \geq 0, \text{ for } 1 \leq i \leq 5$$

$$\text{9 1's, 4 0's, 13 total} \rightarrow \binom{13}{4}$$

Chapter 2

Fundamentals of Mathematical Logic

2.1 Propositions and Related Concepts

The central focus of this chapter is logic, or the science of reasoning. We study the validity of argument. That is, whether a conclusion necessarily follows from the preceding premises. The truth of the final conclusion cannot be determined using logic, only the validity of the argument asserting the final conclusion.

In computer science, we can apply logic to both the design and implementation of hardware and software. In the former, we construct physical circuits, and in the latter we prove the correctness of software.

Let's begin by formally defining the objects of logic.

Definition 2.1.1

A statement or proposition is a sentence that is true or false, but not both.

Example 2.1.2

Here are some statements:

- The Oilers will win the Stanley Cup this year.
- My shirt is green.
- $x + 2 = 7 \rightarrow$ Only if x is fixed, or known.
- For all x, $x + 2 = 7$
- I am tall $\leftarrow$ Not a statement, it is an opinion.

We typically use letters such as p, q, r to represent statements. Statements that cannot be broken down into smaller pieces are called simple statements. New statements can be constructed from existing statements in two ways: using *negation* and using *logical connectives*.

Compound Statement	Symbol	Read	Alternatives
negation	$\sim p$	not p	$\neg p$, $\bar{p}$, p'
conjunction	$p \wedge q$	p and q	$p \cdot q$
disjunction	$p \vee q$	p or q	$p + q$
exclusive or	$p \oplus q$	p xor q	$p \veebar q$
implication	$p \rightarrow q$	if p then q	
biconditional	$p \leftrightarrow q$	p if and only if q	

Truth Tables for negation and the connectives.

p	$\sim p$
F	T
T	F

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
F	F	F	F	F	T	T
F	T	F	T	T	T	F
T	F	F	T	T	F	F
T	T	T	T	F	T	T

Example 2.1.3

Construct a truth table for $(p \vee q) \rightarrow (r \wedge p)$

p	q	r	$p \vee q$	$p \wedge q$	$(p \vee q) \rightarrow (r \wedge p)$
0	0	0	0	0	1
0	0	1	0	0	1
0	1	0	1	0	0
0	1	1	1	0	0
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	1	0	0
1	1	1	1	1	1

Definition 2.1.4

Logical Equivalence : The laws of logic. Two statements s_1 and s_2 are called logically equivalent if and only if the statement s_1 is true (respectively false) whenever the statement s_2 is true (respectively false). We write $s_1 \Leftrightarrow s_2$.
Note: $s_1 \leftrightarrow s_2$ is a statement that is either true or false. We use the symbolism $s_1 \equiv s_2$ or $s_1 \Leftrightarrow s_2$ to denote that $s_1 \leftrightarrow s_2$ is true.

Example 2.1.5

Complete the following truth table:

p	q	$p \vee q$	$\sim (p \vee q)$	$\sim p \vee \sim q$	$\sim p \wedge \sim q$
0	0	0	1	1	1
0	1	1	0	1	0
1	0	1	0	1	0
1	1	1	0	0	0

This table demonstrates one of DeMorgan's Laws.

Proposition 2.1.6

The negation of a conjunction or disjunction is defined by the following equivalences known as DeMorgan's Laws.

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$

Example 2.1.7

Show that $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

p	q	r	$q \vee r$	$p \wedge (q \vee r)$	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Definition 2.1.8

A tautology is a compound statement that is always true for all truth values assignments to its component statements. A contradiction is a compound statement that is always false for all truth values assignments to its component statements.
The symbols t and c denote any tautology and contradiction respectively.

2.2 Common Logical Equivalences

Double Negative Law:	$\sim\sim p \equiv p$
DeMorgan's Laws:	$\sim (p \wedge q) \equiv \sim p \vee \sim q$
	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
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:	$p \wedge t \equiv p$
	$p \vee c \equiv p$
Inverse Laws:	$p \vee \sim p \equiv t$
	$p \wedge \sim p \equiv c$
Domination Laws:	$p \vee t \equiv t$
	$p \wedge c \equiv c$
Absorption Laws:	$p \vee (p \wedge q) \equiv p$
	$p \wedge (p \vee q) \equiv p$
Idempotent Laws:	$p \wedge p \equiv p$
	$p \vee p \equiv p$

Example 2.2.1

Is $p \vee (\sim p \vee \sim (p \wedge q))$ a tautology?

$$
\begin{aligned}
& p \vee (\sim p \vee \sim (p \wedge q)) \\
\equiv\ & p \vee (\sim p \vee (\sim p \vee \sim q)) \\
\equiv\ & p \vee (\sim p \vee \sim p) \vee \sim q \\
\equiv\ & (p \vee \sim p) \vee \sim q \\
\equiv\ & t \vee \sim q \\
\equiv\ & t
\end{aligned}
$$

2.3 Conditional and Biconditional Propositions

In the previous section we introduced the logical connectives $\rightarrow$ and $\leftrightarrow$. We now explore these more detail. In the sentence, "if p, then q", denoted symbolically by "$p \rightarrow q$", the statement p is called the *hypothesis* and q is called the *conclusion*.

Example 2.3.1

Let p, q, and r denote the following:

p: Discrete mathematics is required for computing majors.

q: Linear algebra is offered on Tuesday and Thursday.

r: Jane will take linear algebra

Express each of the following in words:

- $(p \vee q) \rightarrow r$

  If discrete math is required for computer science or linear algebra is offered Tuesday and Thursday**, then** Jane will take Linear Algebra.

- $(p \wedge r) \leftrightarrow q$

  Both discrete math is not required for computer science majors and Jane will take linear algebra, **,if and only if,** Linear Algebra is offered on Tuesday and Thursday.

Example 2.3.2

When is the statement "If you attend all the lectures, then you will pass the course" true and when is it false? In other words, under what conditions could you accuse your professor of lying?

You can only accuse your professor of lying when you attend all the lectures, and still fail.

Example 2.3.3.

Is the statement $(5+2=6) \rightarrow \left(4^2=15\right)$ true or false?

$$\text{Suppose } 5+2=6$$

$$\text{Consider } 4^2 = 4 \times 4 = 4+4+4+4$$

$$= 4+1+1+2+4+4+4$$

$$= 5+2+1+4+4$$

$$= 6+1+4+4$$

$$= 15$$

This is true, but $(5+2=6) \rightarrow \left(4^2=16\right)$ is also true.

Example 2.3.4

Construct a truth table for $p \rightarrow q$ and for $\sim p \vee q$.

p	q	$p \rightarrow q$	$\sim p$	$\sim p \vee q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

Proposition 2.3.5

The statement $p \to q$ is equivalent to $\sim p \vee q$.

The Negation of a Conditional Statement

The negation of $p \to q$ is not a conditional statement. Using $(p \to q) \equiv (\sim p \vee q)$ and DeMorgan's Laws we get the following proposition.

Proposition 2.3.6

The negation of "if p, then q" is logically equivalent to $p \wedge \sim q$. That is,

$$\sim (p \to q) \equiv p \wedge \sim q$$

Example 2.3.7

Negate "If Xiaotang's program compiles, then it is error free."

Xiatoang's program compiles and it is not error free.

The Contrapositive, Converse, and Inverse

Given any conditional statement, $p \to q$, there are four other statements we can define. The equivalence of (some of) these statements is an important tool in developing mathematical proofs.

Definition 2.3.8

The contrapositive of the conditional statement "if p, then q" is

$$\text{if not } q, \text{ then not } p$$

Symbolically:

$$\sim q \to \sim p$$

Proposition 2.3.9

A conditional statement is logically equivalent to its contrapositive.

Proof: We can use a truth table, or ...

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

Q.E.D.

The other statements that are not logically equivalent to a given conditional statement are defined below.

Definition 2.3.10

Suppose a conditional statement of the form "if p, then q" is given.

1. The converse is: if q, then p
2. The inverse is: if not p, then not q

Symbolically:

1. The converse of $p \to q$ is $q \to p$ and
2. The inverse of $p \to q$ is $\sim p \to \sim q$

Proposition 2.3.11

1. A conditional statement and its converse are not logically equivalent.
2. A conditional statement and its inverse are not logically equivalent.
3. The converse and the inverse of a conditional statement are logically equivalent to each other.

Example 2.3.12

Write the converse, inverse, contrapositive, and negation of "If the program compiles, then it is error free."

1. Converse: If the program is error free, then it compiles
2. Inverse: If the program does not compile, then it is not error free
3. Contrapositive: If the positive is not error free, then it does not compile
4. Negation: The program compiles and it is not error free

Example 2.3.13

Write the converse, inverse, and contrapositive, and negation of the following statement: "If Sandra finishes her work, she will go to the basketball game unless it snows."

f: Sandra finishes her work
b: Sandra goes to the basketball game
s: It snows

$$(f \wedge \sim s) \rightarrow b$$

$$\text{or } f \rightarrow (b \vee s)$$

$$\text{or } \sim b \rightarrow (\sim f \vee s)$$

It might be snowing and she still goes to the game, so:

$$f \rightarrow (b \leftrightarrow \sim s)$$

is not quite right.

1. Converse: If Sandra goes to the basketball game, then she finished her work and it is not snowing

$$b \rightarrow (f \wedge \sim s)$$

2. Inverse: If either Sandra doesn't finish her work or it snows, then Sandra doesn't go to the basketball game

$$\sim (f \wedge \sim s) \rightarrow \sim b \equiv (\sim f \vee s) \rightarrow \sim b$$

3. Contrapositive: If Sandra doesn't go to the basketball game, then either she didn't finish her work, or it is snowing

$$\sim b \rightarrow (\sim f \vee s)$$

4. Sandra finishes her work and it doesn't snow, and she doesn't go the basketball game

Definition 2.3.14 : The Biconditional

If p and q are statements, "p only if q" means "if p, then q", or, equivalently, $p \rightarrow q$

Example 2.3.15

You can go out and play only if you finish your homework. Rewrite this in "if-then" form. What does a parent really mean when they say this?

If you go out and play, then you will finish your homework. Parents really mean If you finish your homework, then you will go out and play.

In logic, when we intend a biconditional we must write both if and only if.

Example 2.3.16

Express "For a fixed number n, n is even if and only if $n+2$ is even." using two conditional statements

1. If n is even, then $n+2$ is even and
2. If $n+2$ is even, then n is even

One should note that "p only if q" is not the same "p if q". The words "if and only if" are sometimes abbreviated "iff".

Definition 2.3.17 : Necessary and Sufficient Conditions

If r and s are statement variables:

1. r is a sufficient condition for s means $r \to s$
2. r is a necessary condition for s means $s \to r$

Proposition 2.3.18

The statement r is a necessary condition for s also means "if s, then r."

Proposition 2.3.19

The statement r is a necessary and sufficient condition for s means "r if, and only if, s"

Example 2.3.20

Let n be some fixed integer greater than 3. Is "n is even" a necessary condition for n being a composite number? Is it a sufficient condition? (Write both statements in the "if-then" form.)

n is even is not necessary for n to be composite $(3 \cdot 5 = 15)$

If n is even (and $n > 3$) it is sufficient to say n is composite

$n > 3$, if n is even, then n is composite

2.4 Related Propositions: Inference Logic

Definition 2.4.1

An argument is a sequence of statements. All statements but the final one are called premises (or assumptions or hypotheses). The final statement is called the conclusion. The symbol "$\therefore$", read "therefore", is normally placed just before the conclusion.

Definition 2.4.2

An argument of the form:

$$p_1$$
$$p_2$$
$$p_3$$
$$\vdots$$
$$p_n$$
$$\therefore q$$

Is valid iff the statement form

$$(p_1 \wedge p_2 \wedge p_3 \wedge \cdots \wedge p_n) \rightarrow q$$

is a tautology.
We write

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Rightarrow q$$

read "$p_1 \wedge \cdots \wedge p_n$ implies q" to mean the conditional is a true statement.

Test for Validity

To test an argument for validity

1. Identify the hypotheses and conclusion of the argument.
2. Construct a truth table showing truth values of all the hypotheses and the conclusion.
3. Find the rows (called critical rows) in which all the hypotheses are true.
4. In each critical row determine whether the conclusion of the argument is also true. If in each critical row the conclusion is true, then the argument form is valid. Otherwise, the argument form is invalid.

Example 2.4.3

Show using a truth table that the following argument is valid:

$$p \vee q$$
$$p \rightarrow r$$
$$q \rightarrow r$$
$$\therefore r$$

	p	q	r	$p \vee q$	$p \rightarrow r$	$q \rightarrow r$	r
	0	0	0	0	1	1	
	0	0	1	0	1	1	
	0	1	0	1	1	0	
$\star$	0	1	1	1	1	1	1
	1	0	0	1	0	1	
$\star$	1	0	1	1	1	1	1
	1	1	0	1	0	0	
$\star$	1	1	1	1	1	1	1

This is a valid argument

The textbook contains many standard arguments called rules of inference. We present two very common rules.

Modus Ponens

(from the Latin "method of affirming")

$$p \to q$$
$$p$$
$$\therefore q$$

	p	q	$p \to q$	p	q
	0	0	1	0	
	0	1	1	0	
	1	0	0	1	
$\star$	1	1	1	1	1

This is a valid argument.

Example 2.4.4

If Lucas and Luke are home, then they are playing baseball.
Lucas and Luke are home.
$\therefore$ they are playing baseball

Modus Tollens

(from the Latin "method of denying")

$$p \to q$$
$$\sim q$$
$$\therefore \sim p$$

	p	q	$p \to q$	$\sim q$	$\sim p$
$\star$	0	0	1	1	1
	0	1	1	0	
	1	0	0	1	
	1	1	1	0	

This is a valid argument.

Example 2.4.5

If the x-men are playing then they will win tonight.
The x-men didn't win tonight.
$\therefore$ they didn't play tonight

Common Mistakes

Two common mistakes in constructing arguments are the converse error and the inverse.

Converse Error

$$p \to q$$
$$q$$
$$\therefore p$$

	p	q	$p \to q$	q	p
	0	0	1	0	
$\star$	0	1	1	1	0
	1	0	0	0	
$\star$	1	1	1	1	1

Invalid, since conclusion is false in a critical row

Example 2.4.6

If it is raining, then I won't go into town
I don't go into town
therefore it is raining

Inverse Error

$$p \to q$$
$$\sim p$$
$$\therefore \sim q$$

	p	q	$p \to q$	$\sim p$	$\sim q$
$\star$	0	0	1	1	1
$\star$	0	1	1	1	0
	1	0	0	0	
	1	1	1	0	

Example 2.4.7

If it is raining, then I won't go into town
It is not raining
therefore I will go to town

Our final argument form is extremely common. Essentially, if one wishes to show p is true, we instead show that $\sim p$ cannot be true.

Definition 2.4.8

The Contradiction Rule states that if you can show the supposition that statement p is false leads to a contradiction, then you can conclude p is true. Symbolically:

$$\sim p \to c$$
$$\therefore p$$

Example 2.4.9

Knights and Knaves: An island contains two types of people: knights who always tell the truth and knaves who always lie. You visit the island and are approached by two natives who speak to you as follows:

A says: B is a knight B says: A and I are of opposite type.

What are A and B?

Suppose A is a knight (A is truthful) $\Rightarrow$ B is a knight (truth) $\Rightarrow$ A and B are opposites, but A, B are both knights $\to\leftarrow$ (a contradiction)
Therefore, A is a knave (lying)
$\Rightarrow$ B is a knave

2.5 Predicates and Quantifiers

Definition 2.5.1

A declarative statement is a predicate or open statement if

(a) it contains at least one variable

(b) it is not a statement, and

(c) it becomes a statement when the variables in it are replaced by specific values

Domain

The allowable choices constitue what is called the domain or truth set for the predicate.

Sets of Numbers

Some very common sets of numbers.

Symbol	Set	
$\mathbb{R}$	Real Numbers	
$\mathbb{Q}$	Rational Numbers	
$\mathbb{Z}$	Integers	
$\mathbb{N}$	Natural Numbers	$\{1, 2, 3, 4, 5, \dots\}$
$\mathbb{W}$	Whole Numbers	$\{0, 1, 2, 3, 4, \dots\}$

Example 2.5.2

Let $p(n)$ denote $1 + 2 + 3 + \cdots + n = n(n+1)/2$. Is $p(n)$ a statement? A predicate? What is the domain?

Not a statement

$$n = 1 \quad p(1) : 1 = 1$$
$$n = 2 \quad p(2) : 1 + 2 = \frac{2 \cdot 3}{2} = 3$$

It is a predicate
Domain is $\mathbb{N}$

Example 2.5.3

Determine the truth set for the $p(x)$: "x is a factor of 36" and $q(x)$: "36 is a factor x".

$$p(x) : \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$
$$q(x) : \{36, 72, 108, \dots\}$$
$$= \{36k \mid k \in \mathbb{N}\}$$

Example 2.5.4

Let $p(x)$ denote the predicate "The number $x + 2$ is a prime number". Let $q(x, y)$ denote "The sum $x + y$ is even".

- What are the allowable choices for x in p? $\mathbb{W}$ or $\mathbb{N}$
- What are the allowable choices for x, y in q? $\mathbb{Z}$

Decide whether each of the following statements are true or false.

(a) $p(3)$ true

(b) $p(4)$ false

(c) $q(2, 6)$ true

(d) $\sim q(2, 3)$ true

(e) $q(3, 8)$ false

Hence we can conclude

- For some integers x, $p(x)$ is true
- For some integers x and y, $q(x, y)$ is true
- Yet we also have for some integers x and y, $\sim q(x, y)$ is true

Hence, "for some x and y, $q(x, y)$" and "for some x and y, $\sim q(x, y)$ are not negations of each other."

Quantified Statements

We can change predicates into statements by using quantifiers. Essentially quantifiers tell us which elements of the universe we need to consider.

Definition 2.5.5

The existential quantifier, denoted $\exists$, is read "for some", "there exists", "there is a". The symbols $\exists x, p(x)$ are read as "There exists an x such that $p(x)$"
The statement $\exists x, p(x)$ is true if there is an x that makes $p(x)$ true.

Definition 2.5.6

The universal quantifier, denoted $\forall$, is read "for all", "for any", "for each". The symbols $\forall x, p(x)$, are read as "For all x, $p(x)$".
The statement $\forall x, p(x)$ is true if all allowable values of x make $p(x)$ true.

From our example above, $p(x)$: The number $x + 2$ is prime, $\exists x, p(x)$ is true; e.g. take $x = 3$. Whereas, $\forall x, p(x)$ is false; e.g. take $x = 4$

Example 2.5.7

Let the following predicates have the universe of all real numbers.

$$p(x) : x \geq 0$$
$$q(x) : x^2 \geq 0$$
$$r(x) : x^2 - 25 > 0$$
$$s(x) : x^2 - 3x - 10 = 0$$

Are the following true or false?

(a) $\forall x, p(x)$
False, $x = -1$

(b) $\exists x, p(x)$
True $x = 1$

(c) $\forall x, \sim p(x)$
False, $x = 2$

(d) $\sim (\forall x, p(x))$
True $x = -\frac{1}{2}$

(e) $\forall x\, [p(x) \to q(x)]$
True

(f) $\forall x\, [r(x) \to p(x)]$
False $x = -6$

(g) $\exists x\, [r(x) \to p(x)]$
True

(h) $\forall x\, [s(x) \vee r(x)]$
False $x = 0$

(i) $\forall x\, [s(x) \to p(x)]$
False $x = -2$

(j) $\exists x\,[r(x) \wedge s(x)]$
False, no value makes both statements true

(k) $(\exists x, r(x)) \wedge (\exists x, s(x))$
True $x = 6$, $x = -2$

Negation of a Universal Quantifier

The negation of a statement of the form

$$\forall x, p(x)$$

is not a universally quantified statement. Rather to say that not all values of x make $p(x)$ true is equivalent to saying there is a value that makes $p(x)$ false.

This can be expressed symbolically as:

$$\sim \forall x, p(x) \equiv \exists x, \sim p(x)$$

Example 2.5.8

Negate "All solutions to $x^2 - 3x - 10 = 0$ are positive".

There is a solution to $x^2 - 3x - 10 = 0$, which is not positive.

Negation of an Existential Quantifier

Similar to above, the negation of a statement of the form

$$\exists x, p(x)$$

is not an existentially quantified statement. Rather it is logically equivalent to a statement of the form

$$\sim \exists, p(x) \equiv \forall x, \sim p(x)$$

Example 2.5.9

Negate "Some integers are positive"

All integers are not positive

Universal Conditional Statements

Example 2.5.10

Let $p(x)$ denote "x is a squiare" and $q(x)$ denote "x s a rectangle", with the universe taken as all polygons in the plane. Convert the statement "All squares are rectangles" to symbols and determine its truth value:

$$\forall x, p(x) \rightarrow q(x) \text{ or } \forall x, \sim q(x) \rightarrow \sim p(x)$$

In fact, the following equivalences still exist for Universal Conditional Statements

The original is equivalent to the contrapositive, the converse is equivalent to the inverse

To negate a universal conditional statement we simply apply the rules of negation for universal statements and for conditional statements. For example,

$$\sim (\forall x, p(x) \rightarrow q(x))$$

$$\exists x, \sim (p(x) \rightarrow q(x))$$

$$\exists x, p(x) \wedge \sim q(x)$$

Example 2.5.11

Negate "For all real numbers x, if $x > 2$, then $x^2 > 4$"

There exists a real number x, such that $x > 2$ and $x^2 \leq 4$

Nested Quantifiers

Example 2.5.12

Write the following using symbols and determine if each is true or false.

(a) There are two integers whose sum is even

predicate

$$e(x, y) : x + y \text{ is even}$$

quantified statement

$$\exists x \, \exists y, e(x, y) \text{ or } \exists x, y, e(x, y)$$

truth value

$$\text{true, } x = 1, y = 7$$

(b) Given any integer, there is a second so that their sum is even

predicate

$$e(x, y) : x + y \text{ is even}$$

quantified statement

$$\forall x \, \exists y, e(x, y)$$

truth value

$$\text{true}$$

(c) There exists an integer such that its sum with all other integers is even

predicate

$$e(x, y) : x + y \text{ is even}$$

quantified statement

$$\exists x \, \forall y, e(x, y)$$

truth value

$$\text{false}$$

We can condlude that $(\exists x, \exists y)$, $(\exists y, \exists x)$ and $(\exists x, y)$ all mean the same thing. However, $(\forall x, \exists y)$ and $(\exists y, \forall x)$ do not.

Example 2.5.13

In calculus the idea of a limit is formalized as follows:

$$\lim_{x \to c} f(x) = L \equiv \forall \varepsilon > 0, \exists \delta > 0 \text{ such that } |x - c| \leq \delta \to |f(x) - L| \leq \varepsilon$$

Write the statement that means $\lim_{x \to c} f(x) \neq L$.

$$\sim (\forall \varepsilon > 0, \exists \delta > 0 \text{ such that } |x - c| \leq \delta \to |f(x) - L| \leq \varepsilon)$$

$$\equiv \exists \varepsilon > 0, \forall \delta > 0, \text{ s.t. } \exists x, |x - c| \leq \delta \text{ and } |f(x) - L| > \varepsilon$$

Chapter 3

Fundamentals of Mathematical Proof

3.1 Direct Proof and Counterexample

We can now apply our rules of inference to prove statements about the mathematical objects called the integers.

Definition 3.1.1

Let n be an integer

- n s even if $n = 2k$ for some integer k
- n is odd if $n = 2k + 1$ for some integer k
- $n > 1$ is prime if for all positive integers r and s, $n = rs$ implies $r = 1$ or $s = 1$.
- $n > 1$ is composite if there exists positive integers r and s such that $n = rs$ and $r \neq 1$ and $s \neq 1$

Example 3.1.2

Is 0 even? Is -75 odd?

$$0 = 2 \cdot 0, \text{ so } 0 \text{ is even}$$

$$-75 = 2 \cdot (-38) + 1, \text{ so } -75 \text{ is odd}$$

Example 3.1.3

Is 11 prime? Is 1 prime? Is it true that every number greater than 1 is either prime or composite?

Is 11 prime? Yes, but it is hard to check
Is 1 prime? No!
Is it true that every number greater than 1 is either prime or composite? Yes

$$\begin{aligned} \sim (\text{prime}) &\equiv \sim [\forall r, s \;\; n = rs \to (r = 1 \vee s = 1)] \\ &\equiv \exists r, s \;\; \sim [n = rs \to (r = 1 \vee s = 1)] \\ &\equiv \exists r, s \;\; n = rs \wedge \sim (r = 1 \vee s = 1) \\ &\equiv \exists r, s \;\; n = rs \wedge r \neq 1 \wedge s \neq 1 \\ &\equiv \text{ composite} \end{aligned}$$

Existence Proof - Constructive

Example 3.1.4

Prove $\exists$ an even integer n that can be written as a sum of two primes in two ways.

$$16 = 13 + 3 \qquad 10 = 3 + 7 \qquad 14 = 7 + 7$$
$$16 = 11 + 5 \qquad 10 = 5 + 5 \qquad 14 = 11 + 3$$

Method of Exhaustion

Example 3.1.5

Prove $\forall$ integers n, if n is even and $4 \leq n \leq 12$, then n can be written as a sum of two prime numbers.

$$4 = 2 + 2$$
$$6 = 3 + 3$$
$$8 = 5 + 3$$
$$10 = 5 + 5$$
$$12 = 7 + 5$$

Is this always true? Christian Goldback (1690 - 1764) conjectured that every even integer greater than 2 can be so represented. Verified up to 10^16 but remains open.

Counterexamples

Example 3.1.6

What is required to show that a universal statement is false?
An existence proof.

What does a counter example to a universal conditional look like?
$n =$ ____ and this is why it makes the statement false

Disprove "for all real numbers a and b, if $ab = b^2$, then $a = b$."

$$a = 0,\ b = 1$$
$$1 \cdot 0 = 0^2$$

But, $1 \neq 0$

The Rule of Universal Generalization

Of course, the method of exhaustian works only when the set being checked is finite and fairly small. A powerful technique for proving a universal statement that works regardless of the size of the domain is *The Rule of Universal Generalization.*

The idea is to show that every element of the domain satisfies a certain property by assuming x is a fixed but arbitrary element of the domain and proving that x satisfies the property.

Method of Generalizing from the Generic Particular

1. Express the statement to be proved in the form $\forall x \in D$, if $P(x)$, then $Q(x)$. (This step may be done mentally).
2. Start the proof with a sentence of the form "Suppose x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true."
3. Show that the conclusion $Q(x)$ is true.

Example 3.1.7

Prove: The sum of any two even integers is even.

$\forall x, y$ if x and y are both even, then $x + y$ is even

Proof:
Let x and y be fixed but arbitrary even integers
This means:
$\exists$ an integer k such that $x = 2k$
$\exists$ an integer l such that $y = 2l$
$x + y = (2k + 2l) = 2(k + l)$

Example 3.1.8

Prove if n is even, then n^2 is even.

Let n be a fixed but arbitrary even integer.
This means:
$\exists$ an integer k s.t. $n = 2k$
$n^2 = 4k^2$
$n^2 = 2(2k^2)$
Since $2k^2$ is an integer, n^2 is even.

Example 3.1.9

Prove or disprove: If n is an integer, then $n^2 = n$

Disprove: $n = 2$, then n is an integer, but $2^2 \neq 2$

Example 3.1.10

A number n is rational if there exists integers a and $b \neq 0$ such that $n = \frac{a}{b}$. Prove the sum of the two rationals is rational

Let x and y be fixed but arbitrary rational numbers
This means:
$\exists$ integers a and $b \neq 0$ s.t. $x = \frac{a}{b}$
and $\exists$ integers c and $d \neq 0$ s.t. $y = \frac{c}{d}$
$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad+bc}{bd}$
Hence, $x + y$ is rational since $ad + bc$ is an integer and bd is an integer and $bd \neq 0$ since $b \neq 0$ and $d \neq 0$

Common Errors in Proofs

1. Arguing from examples
2. Using the same letter to mean two different things
3. Jumping to a conclusion
4. Begging the question
5. Misuse of the word *if*

Definition 3.1.11

Let n and d be integers with $d \neq 0$. Then n is divisible by d (written $d|n$ and read d divides n) if $\exists$ an integer k such that $n = dk$.
Alternatively, n is a multiple of d, d is a factor of n, d is a divisor of n, or d divides n

Example 3.1.12

Which of the following are true?

- $3|15$ true, $15 = 3 \cdot 5$
- $15|3$ false $3 = 15 \cdot \frac{1}{5}$ (not an integer)
- $1|7$ true $7 = 1 \cdot 7$
- $\forall n \in \mathbb{Z}, n|n$ false, since $n = 0$ is an exception
- $\forall n \in \mathbb{Z}, n|0$ false, since $d \neq 0$

Example 3.1.13

Prove for all integers a, b, c if $a|b$ and $b|c$, then $a|c$.

Let a, b, c be fixed but arbitrary integers such that $a|b$ and $b|c$
This means:
$\exists$ an integer k s.t. $b = a \cdot k$
and $\exists$ an integer l s.t. $c = b \cdot l$
$c = b \cdot l$
$= (a \cdot k) \cdot l$
$= a \cdot (k \cdot l)$
So $a|c$ since $k \cdot l$ is an integer

Example 3.1.14

Prove or disprove: For all integers a and b. If $a|b$ and $b|a$, then $a = b$

Disprove: $a = 6, b = -6$, then $a|b$ and $b|a$ but $a \neq b$

Incorrect Solution:
Let a, b be fixed but arbitrary integers, s.t. $a|b$ and $b|a$
This means:
$\exists$ an integer k s.t. $b = a \cdot k$
and $\exists$ an integer l s.t. $a = b \cdot l$
$a = b \cdot l = (a \cdot k) \cdot l$ $a \cdot kl \Rightarrow kl = 1$
$k, l = 1$ or $k, l = -1$
$b = a \cdot 1 = a$ or $b = a \cdot (-1) = -a$

Vacuous Proofs

Example 3.1.15

Prove that if $1 + 1 = 3$, then Rupert is a purple cat

True, since $1 + 1 \neq 3$

Trivial Proofs

Example 3.1.16

Show that if n is an even integer then n is divisible by 1

All integers are divisible by 1.

Proofs by Cases

Example 3.1.17

Prove the square of an odd integer has the form $8m + 1$ for some m

$\forall x \in \mathbb{Z}$, if x is odd, then $x^2 = 8m + 1$ for some integer m
Let x be a fixed but arbitrary odd integer. Then, if I divide x by 4, I either get a remainder of 1 or 3.
Case 1: $x = 4k + 1$ for some integer k

$$x^2 = (4k + 1)^2$$
$$= 16k^2 + 8k + 1$$
$$8(2k^2 + k) + 1$$

Since $2k^2 + k$ is an integer, $x^2 = 8m + 1$
Case 2: $x = 4k + 3$ for some integer k

$$x^2 = (4k + 3)^2$$
$$= 16k^2 + 24k + 9$$
$$= 16k^2 + 24k + 8 + 1$$
$$= 8(2k^2 + 3k + 1) + 1$$

Since $2k^2 + 3k + 1$ is an integer, x^2 is of the form $8m + 1$

Example 3.1.18

Use the proof on the previous page to write a program that takes an odd integer n as input, and writes n^2 as $8m + 1$

```
// divcases.cpp
// Carter Clifton
// July 2004

// Small program to demonstrate how a proof by
// division into cases can be turned into an algorithm

#include <iostream>

using namespace std;

int main() {
    // Read an integer
    int n;
    cout << "Enter an odd integer: ";
    cin >> n;

    // Write n as 4q + r
    int q = n / 4; // Compute the quotient and
    int r = n % 4; // remainder when n is divided by 4

    // From our proof, we know if
    // r = 1, then n^2 = 8 * (2 * q^2 + q) + 1;
    // r = 3, then n^2 = 8 * (2 * q^2 + 3 * q + 1) + 1;
    // r = 2 or 4, then n is even, i.e. bad input
    int m;
    switch(r) {
        case 1:
            m = 2 * q * q + q;
            break;
        case 3:
            m = 2 * q * q + 3 * q + 1;
            break;
        default:
            cout << "You did not enter an odd integer." << endl;
```

```
36              exit(1);
37      }
38
39      // Display the results.
40      cout << "You entered " << n << " for which is ";
41      cout << "n^2 = " << n * n << " = 8 * " << m << " + 1 " << endl;
42
43      return 0;
44  }
```

3.2 Indirect Proofs

An example of an indirect proof is argument by contraposition. It is based on the logical equivalence between a statement and its contrapositive.

Method of Proof by Contraposition

- Express the statement to be proven in the form

$$\forall x \in D, P(x) \rightarrow Q(x)$$

  (This step may be done mentally.)

- Rewrite this statement in the contrapositive form

$$\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$$

  (This step may also be done mentally.)

- Prove the contrapositive statement by the method of generalizing from the generic particular

Example 3.2.1

Prove: For all positive integers m and n, if $mn = 1$, then $m = 1$ and $n = 1$

Proof: (by contrapositive)

$$\forall m, n \in \mathbb{Z}^+, m \neq 1 \text{ or } n \neq 1 \rightarrow mn \neq 1$$

Let m and n be fixed but arbitrary positive integers so that $m \neq 1$ or $n \neq 1$
This means either $m > 1$ or $n > 1$
Without loss of generalization (WOLOG) assume $m > 1$

$$mn > 1 \cdot n \geq 1 \cdot 1 = 1 \Rightarrow mn > 1 \Rightarrow mn \neq 1$$

Example 3.2.2

Prove: For all integers n, if n^2 is even, then n is even

Proof: (by contrapositive)

For all integers n if n is odd, then n^2 is odd

Let n be a fixed but arbitrary odd integer.
This means there is an integer k such that $n = 2k + 1$

$$n^2 = (2k+1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$

Since $2k^2 + 2k$ is an integer, n^2 is odd

Example 3.2.3

Prove: For all integers n, n^2 is odd if and only if n is odd.

1. If n^2 is odd, then n is odd
   Contrapositive: If n is even, then n^2 is even.
   Let n be a fixed but arbitrary even integer
   This means that $\exists$ an integer k such that $n = 2k$

   $$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

   Since $2k^2$ is an integer, n^2 is even

2. If n is odd, then n^2 is odd
   Let n be a fixed but arbitrary odd integer
   This means that $\exists$ an integer k such that $n = 2k + 1$

   $$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

   Since $2k^2 + 2k$ is an integer, n^2 is odd

Proof by Contradiction

A slight word of caution is required here. If you are able to prove a statement directly, it is preferable to an indirect proof when both proofs are roughly the same complexity.

Method of Proof by Contradiction

1. Suppose the statement to be proved is false, i.e., assume its negation is true
2. Show that this assumption leads logically to a contradiction
3. Conclude that the statement to be proved is true

There are not clear rules when to apply a direct proof technique or an indirect proof technique. However, if you want to show that a certain object does not have a property or there are no objects with a given property, try a proof by contradiction. In the next section we prove two classical theorems using contradiction.

Two Classical Theorems

We now present two of the most famous (and most ancient) theorems in mathematics. The proofs we present are over 2000 years old! Enjoy.

Example 3.2.4

Prove: The set of prime numbers is infinite.

Proof by contradiction. Assume the set of prime numbers is finite.
This implies there is a largest prime, say N
Consider:

$$\begin{aligned} n &= N! + 1 \\ &= 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (N-1) \cdot N + 1 \end{aligned}$$

Facts about n

- $n > N$

- $N \nmid n$
  $(N-1) \nmid n$
  $(N-2) \nmid n$
  $\vdots$
  $2 \nmid n$
- Since $n > N$, n is composite
- $\Rightarrow \exists$ a prime that divides n

But all primes are between 2 and N (inclusive) and none of them divifde n
A contradiction showing the result.

Example 3.2.5

Prove: $\sqrt{2}$ is irrational.

Proof by contradiction. Assume $\sqrt{2}$ is rational.
This means $\exists a, b \in \mathbb{Z}$ s.t. $b \neq 0$ and $\sqrt{2} = \frac{a}{b}$ so that a and b have no common factors. ($\frac{a}{b}$ is in lowest terms)

$$\sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow a^2 = 2b^2$$

This means a^2 is even, thus a is even.
$\Rightarrow \exists k \in \mathbb{Z}$ so that $a = 2k$

$$a^2 = 2b^2$$
$$(2k)^2 = 2b^2$$
$$4k^2 = 2b^2$$
$$b^2 = 2k^2$$

Since k^2 is an integer, b^2 is even, thus b is even
$\Rightarrow a$ and b share a common factor of 2
A contradiction, showing the result.

3.3 The Pigeonhole Principle

The Pigeonhole Principle states that if n pigeons fly into m holes and $n > m$, then at least one hole has more than one pigeon

Example 3.3.1

If $n+1$ integers are chosen from the set $\{1, 2, 3, \ldots, 2n\}$, then at least one must be odd.

By the PHP:
Pigeons: $n+1$ integers chosen
Pigeon holes: $\{1,2\}, \{3,4\}, \ldots, \{2n-1, 2n\} \quad \leftarrow \quad n$

Since there are more pigeons that pigeonholes, there is a pigeonhole with more than one pigeon in it, and thus one of the integers must be odd

Example 3.3.2

Given a set of 52 distinct integers, show that there must be two chose sum or difference is divisible by 100.

By the PHP:
Pigeons: 52 distinct integers
Pigeon holes (51 total):

$$\{0, 100, -100, 200, -200, \dots\}$$
$$\{1, -1, 99, -99, 101, -101, \dots\}$$
$$\{2, -2, 98, -98, 102, -102, \dots\}$$
$$\vdots$$
$$\{49, -49, 51, -51, \dots\}$$
$$\{50, -50, 150, -150, \dots\}$$

Therefore, since there are more pigeons that pigeonholes, by the PHP two numbers are in the same pigeon hole and their sum or difference is divisible by 100.

Definition 3.3.3

The Generalized Pigeonhole Principle says if n pigeons are placed into m holes and $n > m \cdot k$, then at least one pigeonhole has more than k pigeons (at least $k + 1$ pigeons).

Example 3.3.4

Given 2000 people why must at least 5 have the same birthday?

By the PHP:
Pigeons: 2000 people
Pigeonholes: 366 possible birthdays

$$5 \cdot 366 = 1830 < 2000$$

So by the PHP there must be 6 people who share a birthday

Modular Arithmetic (Bonus)

What is Modular Arithmetic?

$$a \equiv b \mod m$$

This really means a and b have the same remainder when you divide by m

$$(a \equiv b \mod m \Leftrightarrow m|b - a)$$

Congruence Classes

All numbers modulo 3:

$$\{0, 3, -3, 6, -6, \dots\}$$
$$\{1, 4, -2, 7, -5, \dots\}$$
$$\{2, 5, -1, 8, -4, \dots\}$$

These are partitions of the integers.

Example 1

Suppose I want to divide $115 + 287 + 541$ by 5 and find the remainder

$$(115 + 287 + 541) \mod 5$$

$$\equiv 0 + 2 + 1 \equiv 3 \mod 5$$

Properties of Modular Arithmetic

If $a \equiv b \mod m$ and $c \equiv d \mod m$

$$a + c \equiv b + d \mod m$$
$$ac \equiv bd \mod m$$
$$a^n \equiv b^n \mod m$$
$$f(a) \equiv f(b) \mod m \text{ (if } f \text{ is a polynomial)}$$

Example 2

Let $N = 11 \cdot 12 + 13 \cdot 14 + 15 \cdot 16$, what is the units digit of N?

$$N \mod 10$$

$$11 \cdot 12 + 13 \cdot 14 + 15 \cdot 16 \mod 10$$

$$\equiv 1 \cdot 2 + 3 \cdot 4 + 5 \cdot 6 \mod 10$$

$$\equiv 2 + 12 + 30 \equiv 4 \mod 10$$

What is the remainder when you divide by 7?

$$N \mod 7$$

$$11 \cdot 12 + 13 \cdot 14 + 15 \cdot 16 \mod 7$$

$$\equiv (-3) \cdot (-2) + 6 \cdot 0 + 1 \cdot 2 \mod 7$$

$$\equiv 6 + 2 \equiv 1 \mod 7$$

Example 3

Show that $1^n + 8^n - 3^n - 6^n$ is divisible by 10 for all n

$$1^n + 8^n - 3^n - 6^n \mod 10$$

$$1^n 10 \equiv 1 \mod 10$$

$$6^n \equiv 6 \mod 10$$

$$8^1 \equiv 8 \mod 10$$

$$8^2 \equiv 64 \equiv 4 \mod 10$$

$$8^3 \equiv 8^2 \cdot 8 \equiv 4 \cdot 8 \equiv 2 \mod 10$$

$$8^4 \equiv 8^3 \cdot 8 \equiv 2 \cdot 8 \equiv 6 \mod 10$$

$$8^5 \equiv 8^4 \cdot 8 \equiv 6 \cdot 8 \equiv 8 \mod 10$$

pattern: $8, 4, 2, 6$

$$3^1 \equiv 3 \mod 10$$
$$3^2 \equiv 9 \mod 10 \equiv -1 \mod 10$$
$$3^3 \equiv 3^2 \cdot 3 \equiv -1 \cdot 3 \equiv -3 \equiv 7 \mod 10$$
$$3^4 \equiv 3^3 \cdot 3 \equiv -3 \cdot 3 \equiv -9 \equiv 1 \mod 10$$
$$3^5 \equiv 3^4 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \mod 10$$

pattern: $3, 9, 7, 1$

$$1^n + 8^n - 3^n - 6^n \mod 10$$
$$\equiv 1 + 8^n - 3^n - 6 \mod 10$$
$$\equiv 8^n - 3^n - 5 \mod 10$$

if $n \equiv 1 \mod 4$

$$8 - 3 - 5 \equiv 0 \mod 10$$

if $n \equiv 2 \mod 4$

$$4 - 9 - 5 \equiv 0 \mod 10$$

if $n \equiv 3 \mod 4$

$$2 - 7 - 5 \equiv 0 \mod 10$$

if $n \equiv 4 \mod 4$

$$6 - 1 - 5 \equiv 0 \mod 10$$

Algebra

$$2x \equiv 3 \mod 5$$

Method 1

$$2x \equiv 3 + 5 \mod 5$$
$$2x \equiv 8 \mod 5$$
$$x \equiv 4 \mod 5$$

Method 2

$$2 \cdot 0 \equiv 0 \mod 5$$
$$2 \cdot 1 \equiv 2 \mod 5$$
$$2 \cdot 2 \equiv 4 \mod 5$$
$$\star 2 \cdot 3 \equiv 6 \mod 5$$

2 and 3 are inverse numbers

$$\Rightarrow 3 \cdot 2x \equiv 3 \cdot 3 \mod 5$$
$$x \equiv 9 \mod 5$$
$$\equiv 4 \mod 5$$

Example 4

$$\begin{aligned} 20 &\equiv 23 \mod 14 \\ 6x &\equiv 23 \mod 14 \\ 6x &\equiv 23 + 14k \mod 14 \\ 6x - 14k &\equiv 23 \end{aligned}$$

No solution, LHS is even, RHS is odd

3.4 Induction and Recursion

Mathematics is viewed by many as the study of patterns. Often these patterns are predicated by some natural number n. That is, a pattern that depends on some number n

Example 3.4.1

Below are three sequences, find a formula for the n^{th} term.

- $2, 5, 10, 17, 26, \ldots$

$$a_n = a_{n-1} + (2n+1), a_0 = 2$$
$$a_n = n^2 + 1$$

- $4, 8, 16, 32, 64, \ldots$

$$b_n = 2 \cdot b_{n-1}, b_1 = 4$$
$$b_n = 2^{n+1} = 2 \cdot 2^n$$

- $1, 2, 6, 24, 120, \ldots$

$$c_n = n \cdot c_{n-1}, c_1 = 1$$
$$c_n = n!$$

Example 3.4.2

List the first 4 terms of each of the following sequences.

- $a_n = \frac{2^n}{n!}; n \geq 0$

$$\frac{2^0}{0!}, \frac{2^1}{1!}, \frac{2^2}{2!}, \frac{2^3}{3!}$$

- $b_n = \frac{(-1)^n}{n^2+2}; n \geq 0$

$$\frac{1}{2}, \frac{-1}{3}, \frac{1}{6}, \frac{-1}{11}$$

- $c_k = \frac{k}{k+1}; k \geq 5$

$$\frac{5}{6}, \frac{6}{7}, \frac{7}{8}, \frac{8}{9}$$

Definition 3.4.3

Sometimes we want to add or multiply all the members of a sequence. The sum of a sequence in summation form is given by:

$$\sum_{i=1}^{5} a_i = a_1 + a_2 + a_3 + a_4 + a_5$$

and the product of a sequence is given by:

$$\prod_{i=1}^{5} a_i = a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5$$

Example 3.4.4

Find the following:

- $\sum_{n=1}^{5} n^2$

$$1 + 4 + 9 + 16 + 25$$

- $\sum_{n=0}^{5} 2^n$

$$1 + 2 + 4 + 8 + 16 + 32$$

- $\prod_{n=1}^{7} \frac{2}{n}$

$$\frac{2}{1} \cdot \frac{2}{2} \cdot \frac{2}{3} \cdot \frac{2}{4} \cdot \frac{2}{5} \cdot \frac{2}{6} \cdot \frac{2}{7}$$

Mathematical Induction

Mathematical induction is a proof technique that is extremely important and common in both mathematics and computing science. It is used to prove results about open statements quantified over the integers. For example, a statement like "The program is correct after n iterations of the loop" is proved by assuming the program is correct after $n-1$ iterations. Hence, we need only to analyze one step of the program. Recursive algorithms are usually analyzed using induction

Theorem 3.4.5

Principle of Mathematical Induction: Let $S(n)$ denote an open mathematical statement that involves one or more occurences of the variable n which represents a positive integer. Suppose

(a) $S(1)$ is true (Basis step); and

(b) whenever $S(k)$ is true (for some fixed but arbitrary $k \in \mathbb{Z}^+$), then $S(k+1)$ is true. (Inductive step)

Then the statement

$$\forall \text{ integers } n \geq 1, S(n)$$

is true.

The basis step that starts at $n = 1$, could start at any fixed integer. When we establish statement 2, we assume $S(k)$ is true and we prove $S(k+1)$ is true too. The supposition that $S(k)$ is true called the induction hypothesis.

Example 3.4.6

Use mathematical indution to prove that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}, \text{ for all integers } n \geq 1$$

1. Basis: $n = 1$

$$\text{LHS} = 1^2 = 1 \quad \text{RHS} = \frac{1(1+1)(2(1)+1)}{6}$$

2. Induction Hypothesis: Suppose for some fixed but arbitrary $k \geq 1$ that

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

3. Induction Step: Let $n = k + 1$ to show $1^2 + 2^2 + \cdots + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$

$$\begin{aligned}
\text{LHS} &= 1^2 + 2^2 + \cdots + (k+1)^2 \\
&= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= (k+1)\left[\frac{2k^2+k}{6} + \frac{6k+6}{6}\right] \\
&= (k+1)\left[\frac{2k^2+7k+6}{6}\right] \\
&= \frac{(k+1)(k+2)(2k+3)}{6} = \text{RHS}
\end{aligned}$$

4. Conclusion: By the PMI, for all integers $n \geq 1$

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Example 3.4.7

Use mathematical induction to prove that any postage of 8 cents or more can be constructed using 3 cent and 5 cent stamps.

1. Basis: 8 cents = 3¢ + 5¢ stamps
2. Induction Hypothesis: Suppose for some fixed but arbitrary $k \geq 8$, I can make k¢ in postage with 3¢ and 5¢ stamps
   $\exists$ integers a, b s.t. $k = 5a + 3b$, $a, b \geq 0$
3. Induction Step: Let $n = k + 1$ (To show that $(k+1)$¢ can be constructed from 3¢ and 5¢ stamps)
   - Case 1: If $a > 0$, then removing one 5¢ stamp and adding 2 3¢ stamps creates $(k+1)$¢
   - Case 2: If $a = 0$, then $b \geq 3$ (since $k \geq 8$). Remaining 3 3¢ stamps and adding 2 5¢ stamps gives $(k+1)$¢ of postage
4. Conclusion: By the PMI, any postage of 8¢ or more cna be constructed using 3¢ and 5¢ stamps

Example 3.4.8

Let $S(k)$ denote $\sum_{i=0}^{k} i = \left(k^2 + k + 1\right)/2$. Show that $S(k) \Rightarrow S(k+1)$ for all $k \geq 0$. Then show that $S(k)$ is not true for any k.

Assume for some fixed but arbitrary $k \geq 0$,

$$\sum_{i=0}^{k} i = 0 + 1 + 2 + \cdots + k = \frac{(k^2 + k + 1)}{2}$$

to show $S(k+1)$

$$\sum_{i=0}^{k+1} i = \frac{(k+1)^2 + (k+1) + 1}{2} = \frac{k^2 + 3k + 3}{2}$$

$$\begin{aligned}\text{LHS} = \sum_{i=0}^{k+1} i &= 0 + 1 + 2 + \cdots + (k+1) \\ &= [0 + 1 + 2 + \cdots + k] + (k+1) \\ &= \frac{k^2 + k + 1}{2} + (k+1) \\ &= \frac{k^2 + k + 1}{2} + \frac{2k+2}{2} = \frac{k^2 + 3k + 3}{2} = \text{RHS}\end{aligned}$$

RHS of $S(k)$

$$= \frac{k^2 + k + 1}{2} = \frac{k(k+1)}{2} + \frac{1}{2}$$

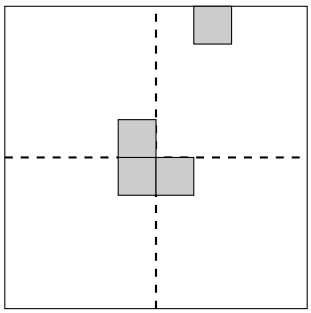
k or $(k+1)$ is even, so $k(k+1)$ is even, so $\frac{k(k+1)}{2}$ is an integer, so $\left(\frac{k(k+1)}{2} + \frac{1}{2}\right)$ is never an integer LHS: $\sum_{i=0}^{k} i$ is a sum of integers, so it is an integer

Example 3.4.9

Consider a chessboard of size $2^n \times 2^n$ with one square removed. Prove it can be tiled with "L" shaped tile consisting of 3 squares.

Proof (by induction)

$n = 1 \Rightarrow$ a 2×2 chessboard with one square removed is just an L-shaped tile. Assume for some fixed but arbitrary $k \geq 1$ a $2^k \times 2^k$ chessboard with one square removed can be tiled with a L-shaped tiles consisting of 3 squares. Consider a $2^{k+1} \times 2^{k+1}$ chessboard with 1 square removed, so break this chessboard into 4 $2^k \times 2^k$ chessboards (shown in the figure below). One of these has a square removed and so by induction I can tile it using L-shaped tiles. Then place a single tile on the intersection of the other 3 as shown so it covers one square of each. Induction implies each of these remaining three can be tiled with L-shaped tiles.



Example 3.4.10

Prove by induction $7^n - 2^n$ is divisble by 5 for $n \geq 1$

Proof (by induction)

- Basis: $n = 1$ $7^1 - 2^1 = 5$, $5|5$
- IH: Assume for a fixed but arbitrary $k \geq 1$, $7^k - 2^k$ is divisible by 5 ($5|7^k - 2^k$)

$$\exists l \in \mathbb{Z} \text{ s.t. } 5l = 7^k - 2^k$$

- IS: $n = k + 1$ (need to show $5|7^{k+1} - 2^{k+1}$)

$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7(7^k) - 2(2^k) \\ &= 5(7^k) + 2(7^k) - 2(2^k) \\ &= 5(7^k) + 2(7^k - 2^k) \\ &= 5(7^k) + 2(5l) \\ &= 5\left[7^k + 2l\right] \end{aligned}$$

  Since $7^k + 2l$ is an integer, $5|7^n - 2^n$

- Conclusion: Therefore by the PMI, $\forall n \geq 1 \in \mathbb{Z}, 5|7^n - 2^n$

Theorem 3.4.11

Principle of Mathematical Induction - Alternative Form Let $S(n)$ denote an open mathematical statement that involves one or more occurences of the variable n, which represents a positive integer. Suppose $n_0, n_1 \in \mathbb{Z}$ with $n_0 \leq n_1$ and further suppose

(a) $S(n_0), S(n_0 + 1), S(n_0 + 2), \ldots, S(n_1)$ are true; and (Basis step)

(b) whenever $S(n_0), S(n_0 + 1), \ldots, S(k - 1), S(k)$ is true (for some fixed but arbitrary $k \geq n_1 \in \mathbb{Z}$), then $S(k + 1)$ is true. (Inductive step)

Then the statement

$$\forall \text{ integers } n \geq n_0, S(n)$$

is true. The supposition that $S(i)$ is true for all integers i with $n_0 \leq i \leq k$ in statement 2 is again called the induction hypothesis.

Example 3.4.12

Prove that every positive integer greater than 1 is either a prime number of the product of primes.

- Basis: $n = 2$, 2 is prime
- IH: Assume for a fixed but arbitrary $k \geq 2$, for all i, $2 \leq i \leq k$. i is either a prime number or a product of primes
- IS: Let $n = k + 1$
  - Case 1: $k + 1$ is prime
  - Case 2: $k + 1$ is composite

    $$\exists r, s \in \mathbb{Z} \text{ s.t. } k + 1 = r \cdot s,\ r, s > 1$$

    Clearly $r, s > k$, so r, s are either primes or products of primes, so $k + 1 = r \cdot s$ is a product of primes
- By PMI, every positive integer > 1 is either a prime or a product of primes

Example 3.4.13

Let $a_0 = 1, a_1 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq 2$. Prove that $a_n \leq \left(\frac{7}{4}\right)^n$.

- Basis:

$$n = 1 \quad a_0 = 1 \leq \left(\frac{7}{4}\right)^0 = 1$$

$$n = 2 \quad a_1 = 1 \leq \left(\frac{7}{4}\right)^1 = \frac{7}{4}$$

- IH: Assume for a fixed but arbitrar $k \geq 1$, for all i, $0 \leq i \leq k$,

$$a_i \leq \left(\frac{7}{4}\right)^i$$

- IS: Let $n = k + 1$ (to show: $a_{k+1} \leq \left(\frac{7}{4}\right)^{k+1}$)

$$\begin{aligned} a_{k+1} = a_k + a_{k-1} &\leq \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} \\ &= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}+1\right) = \left(\frac{7}{4}\right)^{k+1} \cdot \left(\frac{11}{4}\right) \\ = \left(\frac{7}{4}\right)^{k-1}\left(\frac{44}{16}\right) &\leq \left(\frac{7}{4}\right)^{k-1}\left(\frac{49}{16}\right) \leq \left(\frac{7}{4}\right)^{k+1} \end{aligned}$$

- Conclusion: By PMI, $\forall n \geq 0, a_n \leq \left(\frac{7}{4}\right)^n$

Example 3.4.14

Alternative proof that any postage of eight or more cents can be constructed using 3¢ and 5¢ stamps.

- Basis:

$$n = 8 = 3¢ + 5¢ \text{ stamps}$$

$$n = 9 = 3 \;\; 3¢ \text{ stamps}$$

$$n = 10 = 2 \;\; 5¢ \text{ stamps}$$

- IH: Assume for some fixed but arbitrary $k \geq 11$ for all i, $8 \leq i \leq k$, postage of $i¢$ can be constructed using 3¢ and 5¢ stamps
- IS: Let $n = k + 1$, since $k \geq 10$, $k + 1 \geq 11$ and $(k + 1) - 3 \geq 8$, $(k + 1) - 3¢$ in postage can be constructed using 3¢ and 5¢ stamps. Adding a 3¢ stamp gives $(k + 1)¢$ in postage.

Definition 3.4.15

Another version of mathematical induction is the following:

The Well-Ordering Principle: Any nonempty subset of $\mathbb{Z}^+$ contains a smallest element.

In fact, one of the formal axioms used to define the integers is the Well-Ordering Principle. It is equivalent to both forms of Matheatical Induction. Either form can be taken as an axiom, in whic the WOP becomes a theorem (or consequence of the axioms).

Chapter 4

Set Theory

4.1 Basic Definitions of Set Theory

When we study the formal system of set theory we must begin with some primative terms. The words set, element and membership are undefined terms. They are the foundation from which we begin. These terms play the same role as true, false and sentence in logic. Intuitively, a set is a well-defined collection of objects. The objects in the collection are called members or elements of the set.

What does well-defined mean? For every object, it is either in the set or not in the set and there are clear rules around it.

Example 4.1.1

- Do the prime numbers form a set?

  Yes

- Do the interesting numbers form a set?

  Interesting $\rightarrow$ Do we have a clear definition?

- Do the sets that do not contain themselves form a set?

  Not well-defined

Symbolically, we use capital letters $A, B, C, \ldots$ to denote sets and we use lower case letters $a, b, c, \ldots$ to represent elements. One way to define a set is to list its elements between braces: $\{\}$

Example 4.1.2

Let $A = \{a, b, c\}$ be the set with three elements, a, b, and c.

Notation:

- $a \in A$ means a is an element of the set A
- $y \notin A$ means y is not an element of the set A

Again the concept of a set being well-defined means that for a particular x and A, $x \in A$ is a statement. It is also important to note that all of the following are the same set.

$$\{a, b, c\}, \{b, c, a\}, \{a, b, a, a, c, b, a\}$$

Another way to define a set is to use set builder notation. We write

$$\{x | \text{ (open) statement about } x\}$$

read "the set of all elements x such that the statement about x is true." We can also restrict our attention to the elements of some set S that make the set true:

$$\{x \in S | \text{ (open) statement about } x\}$$

Example 4.1.3

Let $\mathbb{Z}$ denote the set of integers. Then $A = \{x \in \mathbb{Z} | -2 \leq x \leq 2\}$ describes the set $A = \{-2, -1, 0, 1, 2\}$. We can also define this by $A = \{x | x \in \mathbb{Z} \wedge -2 \leq x \leq 2\}$

Example 4.1.4

What is $A = \{x | -2 \leq x \leq 2\}$?

The closed interval $[-2, 2]$

When working with sets, we first agree on a universe of discourse, $\mathcal{U}$, i.e. a set from which the elements of A are to be chosen. In the above examples, if $\mathcal{U} = \mathbb{R}$, then $A = [-2, 2]$. If $\mathcal{U} = \mathbb{N}$, then $A = \{1, 2\}$

Example 4.1.5

Let $\mathcal{U} = \mathbb{Z}^+$, the set of positive integers.

$$A = \left\{x^2 \in \mathcal{U} | x^2 < 25\right\} = \left\{x^2 | x \in \mathcal{U}, x^2 < 25\right\} = \left\{x^2 | x \in \mathcal{U} \wedge x^2 < 25\right\} = \{1, 4, 9, 16\}$$

$$B = \{3y | y \in \mathcal{U}, y < 10\} = \{3, 6, 9, 12, 15, 18, 21, 24, 27\} = \{3, 6, 9, \ldots, 27\}$$

$$C = \{2z | z \in \mathcal{U}\} = \{2, 4, 6, \ldots\}$$

Note: A and B are examples of finite sets; whereas, C is an example of an infinite set. The cardinality or size of a finite set S, denoted $|S|$ or $n(S)$, is the number of elements in the set. In the above example,

$$|A| = 4 \text{ and } |B| = 9$$

Some Common Sets

$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N} = \mathbb{Z}^+$, $\mathbb{Z}^-$, and $\mathbb{W}$

Definition 4.1.6

Subsets: Let C, D be sets from a universe $\mathcal{U}$. We say that C is a subset of D, and write $C \subseteq D$, if every element of C is an element of D. If D contains an element that is not in C, then we say C is a proper subset of D, and we write $C \subset D$ or $C \subsetneq D$

Example 4.1.7

Given $A = \{1, 2, 3\}$, $B = \{3, 1, 2\}$, $C = \{1, 2, 3, 5, 7, 9\}$ and $D = \{1, 3, 5, 9\}$, determine if the following statements are true or false.

(a) $A \subseteq B$ and $B \subseteq A$ True

(b) $D \subset C$ True

(c) $A \subset B$ False

(d) $A \subseteq A$ True

(e) $A \subset C$ True

(f) $D \supseteq B$ False

(g) $D \nsubseteq D$ True

(h) $C \subseteq C$ True

Note:

(a) $S \subset T \Rightarrow S \subseteq T \wedge \exists x, x \in T \wedge x \notin S$

(b) For finite sets S, T, $S \subseteq T \Rightarrow |S| \leq |T|$ and $S \subset T \Rightarrow |S| < |T|$

(c)

$$\begin{aligned} S \nsubseteq T &\Leftrightarrow \sim (\forall x, x \in S \rightarrow x \in T) \\ &\Leftrightarrow \exists x, x \in S \wedge x \notin T \end{aligned}$$

Example 4.1.8

Let $\mathcal{U} = \{1, 2, 3, 4, 5, \{1\}, \{1, 2\}, \{1, 2, 3, 4, 5\}\}$. Then $|\mathcal{U}| = 8$

(a) If $A = \{1, 2\}$, then $|A| = 2$; $A \subseteq \mathcal{U}$; $A \subset \mathcal{U}$; $A \in \mathcal{U}$

(b) $|\{A\}| = 1$; $\{A\} \subseteq \mathcal{U}$; $\{A\} \subset \mathcal{U}$; $\{A\} \notin \mathcal{U}$

(c) Let $B = \{1, 3, \{1, 2\}\}$. Then $|B| = 3$; $A \nsubseteq B$; $A \in B$; $\{A\} \subseteq B$; $\{A\} \in B$.

Definition 4.1.9

Equal sets: The sets A and B are equal, denoted $A = B$ if every element of A belongs to B and every element of B belongs to A. Symbolically:

$$A \subseteq B \wedge B \subseteq A$$

Example 4.1.10

Let A and B be sets. Then

$$\begin{aligned} A \neq B &\Leftrightarrow \sim (A \subseteq B \wedge B \subseteq A) \\ &\Leftrightarrow A \nsubseteq B \vee B \nsubseteq A \\ &\Leftrightarrow (\exists x \in A, x \notin B) \vee (\exists x, x \in B \wedge x \notin A) \end{aligned}$$

Example 4.1.11

Let $S = \{n \in \mathbb{Z} | n = 3m + 1 \text{ for some } m \in \mathbb{Z}\}$ and let $T = \{n \in \mathbb{Z} | n = 3m - 5 \text{ for some } m \in \mathbb{Z}\}$. Are S and T equal?

$$S = \{1, 4, 7, 10, 13, \ldots, -2, -5, -8, \ldots\}$$
$$T = \{-5, -2, 1, 4, 5, 7, \ldots, -8, -11, \ldots\}$$

Yes, S and T are equal.

$S \subseteq T$
$(\forall x,$ if $x \in S$ then $x \in T)$
Let $x \in S$
$\Rightarrow \exists$ some $m \in \mathbb{Z}$ s.t.
$x = 3m + 1$
$x = 3m + 1 - 6 + 6$
$x = 3(m + 2) - 5$
Since $m + 2 \in \mathbb{Z}, x \in T$

$T \subseteq S$
Let $x \in T$
$\Rightarrow \exists$ some $m \in \mathbb{Z}$ s.t.
$x = 3m - 5$
$x = 3m - 5 + 6 - 6$
$x = 3(m - 2) + 1$
Since $m - 2 \in \mathbb{Z}, x \in S$

On Proving Sets are Equal

Normally to prove $A = B$, we prove $A \subseteq B$, and then prove $B \subseteq A$. This is accomplished using a proof of the following form:

$$\begin{array}{cc} A \subseteq B & B \subseteq A \\ \text{Let } x \in A & \text{Let } x \in B \\ \vdots & \vdots \\ \Rightarrow x \in B & \Rightarrow x \in A \end{array}$$

By above, to show $A \neq B$, it suffices to give an element in A but not in B or an element in B but not in A.

Set Operations

Suppose "$\bullet$" denotes a binary operation on a set S and, $\forall a, b \in S, a \bullet b \in S$. Then the set S is said to be closed under the binary operation "$\bullet$". For example, if a and b are positive integers, then $a + b$ is a positive integer. Thus, $\mathbb{Z}^+$ is closed under the binary operation "$+$". Note that $\mathbb{Z}^+$ is closed under $\times$ and it is not closed under $-$ nor is it closed under $\div$.

Definition 4.1.12

For sets $A, B \subseteq \mathcal{U}$ we define the following—

(a) The union of A and B is

$$A \cup B = \{x | x \in A \text{ or } x \in\}$$

(b) The intersection of A and B is

$$A \cap B = \{x | x \in A \text{ and } x \in B\}$$

(c) For a set $A \subseteq \mathcal{U}$, the complement of A, denoted $\mathcal{U} - A$ or $\bar{A}$ or A^c, is given by

$$A^c = \{x \in \mathcal{U} | x \notin A\}$$

(d) For $A, B \subseteq \mathcal{U}$, the relative complement of A in B, denoted by $B - A$ is given by

$$B - A = \{x \in B | x \notin A\} = B \cap A^c$$

(e) The symmetric difference of A and B is $A \triangle B =$

$$\begin{aligned} \{x | x \in A \text{ xor } x \in B\} &= (A \cup B - A \cap B) \\ &= (A \cap B^c) \cup (B \cap A^c) \end{aligned}$$

Note: For all $A, B \subseteq \mathcal{U}, A \cup B, A \cap B, A \triangle B \subseteq \mathcal{U}$. Hence, the collection of sets with universe $\mathcal{U}$ is closed under $\cup$, $\cap$, $\triangle$.

Example 4.1.13

Let $\mathcal{U} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, let $A = \{0, 2, 4, 7\}$, $B = \{1, 2, 5, 7, 8\}$, and $C = \{1, 3, 8\}$.

(a) $A \cup B = \{0, 1, 2, 4, 5, 7, 8\}$

(b) $A \cap B = \{2, 7\}$

(c) $A \cap C = \{\} = \emptyset$

(d) $B \triangle C = \{2, 3, 5, 7\}$

(e) $A - B = \{0, 4\}$

Definition 4.1.14

Cartesian Products: For sets, $A, B \subseteq \mathcal{U}$, the Cartesian Product or ??? of A and B is denoted by $A \times B$ and equals

$$\{(x, y)|x \in A, y \in\}$$

The elements of $A \times B$ are called ordered pairs.

More generally, if $A_1, A_2, \ldots, A_n$ are sets we define:

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n)|x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n\}$$

$A_1 \times A_2 \times \cdots \times A_n$ is called the Cartesian product of $A_1, A_2, \ldots, A_n$; the elements of $A_1 \times A_2 \times \cdots \times A_n$ are ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$. Given two n-tuples, we have $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ if $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$.

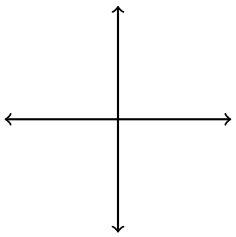
Example 4.1.15

1. Let $A = \{a, b\}$, $B = \{x, y, z\}$ and $C = \{1\}$
   (a) $A \times B = \{(a, x), (a, y), (a, z), (b, x), (b, y), (b, z)\}$
   (b) $A \times (B \times C) = \{(a, (x, 1)), (a, (y, 1)), (a, (z, 1)), (b, (x, 1)), (b, (y, 1)), (c, (z, 1))\}$
   $(B \times C) = \{(x, 1), (y, 1), (z, 1)\}$
   (c) $A \times B \times C = \{(a, x, 1), (a, y, 1), (a, z, 1), (b, x, 1), (b, y, 1), (b, z, 1)\}$
   (d) $(A \cup B) \times C = \{(a, 1), (b, 1), (x, 1), (y, 1), (z, 1)\}$
   $(A \cup B) = \{a, b, x, y, z\}$
2. $A = \{x \in \mathbb{Z}^+|x < 7\}$, $B = \{x \in \mathbb{Z}||x - 2| < 4\}$, $C = \left\{x \in \mathbb{R}|x^3 - 4x = 0\right\}$
   (a) $A = \{1, 2, 3, 4, 5, 6\}$
   (b) $B = \{-1, 0, 1, 2, 3, 4, 5\}$
   (c) $C = \{-2, 0, 2\}$
   (d) $(C - B) \times A = \{(-2, 1), (-2, 2), (-2, 3), (-2, 4), (-2, 5), (-2, 6)\}$
   $(C - B) = \{-2\}$

Example 4.1.16

What is $\mathbb{R} \times \mathbb{R}$?

The cartesian plane



Observations about this Product

(a) $A \times B \neq B \times A$ in general

(b) For finite sets, if $|A| = n$ and $|B| = m$, then $|A \times B| = nm$

(c) In database language, the cross join in SQL is the cartesian product of two tables

Definition 4.1.17

The Empty Set: The empty set or null set denoted by the symbols $\emptyset$ or $\{\}$ is the set containing no elements.

Note: $|\emptyset| = 0$ but $|\{\emptyset\}| = 1$

Theorem 4.1.18

Let $A \subseteq \mathcal{U}$ of some universe $\mathcal{U}$. Then $\emptyset \subseteq A$, and if $A \neq \emptyset$, then $\emptyset \subset A$.

Proof: Let $x \in \emptyset$, this is false, so vaccuously this implies $x \in A$, hence $\emptyset \subseteq A$. And hence if $\emptyset \neq A$, then $\emptyset \subset A$

Corollary 4.1.19

The empty set is unique.

Proof (by contradiction): Suppose the empty set, $\emptyset$ is not unique. Then there is a second empty set, say E. By the theorem $\emptyset \subseteq E$ and $E \subseteq \emptyset$ hence $\emptyset = E$, a contradiction that E is a second empty set showing the result.

4.2 Properties of Sets

Theorem 4.2.1

If A and B are sets, then $A \cap B \subseteq A \subseteq A \cup B$

Proof:

1. $A \cap B \subseteq A$
   Let $x \in A \cap B$
   $\Rightarrow x \in A \wedge x \in B$
   $\Rightarrow x \in A$
2. $A \subseteq A \cup B$
   Let $x \in A$
   $\Rightarrow x \in A \vee x \in B$
   $\Rightarrow x \in A \cup B$

Theorem 4.2.2

Let $A, B, C \subseteq \mathcal{U}$

(a) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$

(b) If $A \subset B$ and $B \subseteq C$, then $A \subset C$

(c) If $A \subseteq B$ and $B \subset C$, then $A \subset C$

(d) If $A \subset B$ and $B \subset C$, then $A \subset C$

Proof (a): Suppose $A \subseteq B$ and $B \subseteq C$

To show: $A \subseteq C$
Let $x \in A$
$\Rightarrow x \in B$ (since $A \subseteq B$)
$\Rightarrow x \in C$ (since $B \subseteq C$)

The Laws of Set Theory

Let A, B, and C be subsets of a universe $\mathcal{U}$.

1. Commutative Laws:
$$A \cap B = B \cap A \text{ and } A \cup B = B \cup A$$
2. Associative Laws:
$$(A \cap B) \cap C = A \cap (B \cap C) \text{ and } (A \cup B) \cup C = A \cup (B \cup C)$$
3. Distributive Laws:
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \text{ and } A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
4. Identity Laws:
$$A \cap \mathcal{U} = A \text{ and } A \cup \emptyset = A$$
5. Double Complement Law:
$$(A^c)^c = A$$
6. Idempotent Laws:
$$A \cap A = A \text{ and } A \cup A = A$$
7. DeMorgan's Laws:
$$(A \cup B)^c = A^c \cap B^c \text{ and } (A \cap B)^c = A^c \cup B^c$$
8. Domination Laws:
$$A \cup \mathcal{U} = \mathcal{U} \text{ and } A \cap \emptyset = \emptyset$$
9. Absorption Laws:
$$A \cup (A \cap B) = A \text{ and } A \cap (A \cup B) = A$$
10. Alternate Representation for Set Difference:
$$A - B = A \cap B^c$$
11. Inverse Laws:
$$A \cup A^c = \mathcal{U} \text{ and } A \cap A^c = \emptyset$$

Note the similarity to the Laws of Logic. In many instances these laws are similar to the Laws of Arithmetic with "$\cup$" playing the role of "$+$" and with "$\cap$" playing the role of "$\times$". There are, however, several differences.

Sample Proof of DeMorgan's Law

$$(A \cup B)^c = A^c \cap B^c$$

1. $(A \cup B)^c \subseteq A^c \cap B^c$

   Let $x \in (A \cup B)^c$
   $\Rightarrow x \notin A \cup B$
   $\Rightarrow \sim (x \in A \vee x \in B)$
   $\Rightarrow x \notin A \wedge x \notin B$
   $\Rightarrow x \in A^c \wedge x \in B^c$
   $\Rightarrow x \in A^c \cap B^c$
2. $A^c \cap B^c \subseteq (A \cup B)^c$

   Let $x \in A^c \cap B^c$
   $\Rightarrow x \in A^c \wedge x \in B^c$
   $\Rightarrow x \notin A \wedge x \notin B$
   $\Rightarrow \sim (x \in A \vee x \in B)$
   $\Rightarrow x \notin A \cup B$
   $\Rightarrow x \in (A \cup B)^c$

Example 4.2.3

Simplify the expression $(A \cup B)^c \cap (B - A)^c$

$$\begin{aligned}
&(A \cup B)^c \cap (B - A)^c \\
&= (A^c \cap B^c) \cap (B \cap A^c)^c \\
&= A^c \cap B^c \cap (B^c \cup A) \\
&= A^c \cap B^c
\end{aligned}$$

Theorem 4.2.4

For any sets $A, B, C \subseteq \mathcal{U}$

(a) $A \times (B \cap B) = (A \times B) \cap (A \times C)$

(b) $A \times (B \cup B) = (A \times B) \cup (A \times C)$

(c) $(A \cap B) \times C = (A \times C) \cap (B \times C)$

(d) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

Proof of (c)

$$(A \cap B) \times C = (A \times C) \cap (B \times C)$$

1. $(A \cap B) \times C \subseteq (A \times C) \cap (B \times C)$

   Let $(x, y) \in (A \cap B) \times C$
   $\Rightarrow x \in (A \cap B) \wedge y \in C$
   $\Rightarrow x \in A \wedge x \in B \wedge y \in C$
   $\Rightarrow x \in A \wedge y \in C \wedge x \in B \wedge y \in C$
   $\Rightarrow (x, y) \in A \times C \wedge (x, y) \in B \times C$
   $\Rightarrow (x, y) \in (A \times C) \cap (B \times C)$

2. $(A \times C) \cap (B \times C) \subseteq (A \cap B) \times C$

   Let $(x, y) \in (A \times C) \cap (B \times C)$
   $\Rightarrow (x, y) \in (A \times C) \wedge (x, y) \in (B \times C)$
   $\Rightarrow x \in A \wedge y \in C \wedge x \in B \wedge y \in C$
   $\Rightarrow x \in A \wedge x \in B \wedge y \in C$
   $\Rightarrow x \in (A \cap B) \wedge y \in C$
   $\Rightarrow (x, y) \in (A \cap B) \times C$

Definition 4.2.5

For any universe $\mathcal{U}$ and any sets $A, B \subseteq \mathcal{U}$, the following statements are equivalent:

(a) $A \subseteq B$

(b) $A \cup B = B$

(c) $A \cap B = A$

(d) $B^c \subseteq A^c$

Proof:

1. $(a) \Rightarrow (b)$
   Suppose $A \subseteq B$ to show $A \cup B = B$

(a) $A \cup B \subseteq B$

$$\text{Let } x \in (A \cup B)$$
$$\Rightarrow x \in A \vee x \in B$$
$$\text{if } x \in B \checkmark$$
$$\text{if } x \in A, \text{ then } x \in B$$
$$\text{since } A \subseteq B$$
$$\Rightarrow x \in B \text{ in both cases}$$

(b) $B \subseteq A \cup B$

$$B \subseteq A \cup B$$
$$\text{Let } x \in B$$
$$x \in A \vee x \in B$$
$$x \in (A \cup B)$$

2. $(b) \Rightarrow (c)$
Suppose $A \cup B = B$ to show $A \cap B = A$

(a) $(A \cap B) \subseteq A$

$$\text{Let } x \in (A \cap B)$$
$$\Rightarrow x \in A \wedge x \in B$$
$$\Rightarrow x \in A$$

(b) $A \subseteq (A \cap B)$

$$\text{Let } x \in A$$
$$x \in A \vee x \in B$$
$$x \in (A \cup B)$$
$$x \in B$$
$$x \in A \wedge x \in B$$
$$x \in (A \cap B)$$

3. $(c) \Rightarrow (a)$
Suppose $A \cap B = A$ to show $A \subseteq B$
Let $x \in A$ since $A = A \cap B$
$\Rightarrow x \in (A \cap B)$
$\Rightarrow x \in A \wedge x \in B$
$\Rightarrow x \in B$

4. $(a) \Leftrightarrow (d)$
$A \subseteq B$
$\Leftrightarrow$ if $x \in A$ then $x \in B$
$\Leftrightarrow$ if $x \notin B$ then $x \notin A$
$\Leftrightarrow$ if $x \in B^c$ then $x \in A^c$
$\Leftrightarrow B^c \subseteq A^c$

Power Sets

Example 4.2.6

Determine all of the subsets of $\{1, 2, 3\}$.

Method 1: List all the subsets

0-elements	1-elements	2-elements	3-elements
$\emptyset$	$\{1\}$	$\{1, 2\}$	$\{1, 2, 3\}$
	$\{2\}$	$\{2, 3\}$	
	$\{3\}$	$\{3, 1\}$	

Method 2: Encode each subset as a binary string of length 3 and list all possible binary strings.

000	100
001	101
010	110
011	111

Total Number: 8

Definition 4.2.7

If A is a set from a universe $\mathcal{U}$, the power set of A, denoted $\mathcal{P}$ is the collection (or set) of all subsets of A.

Example 4.2.8

(a) $\mathcal{P}(\{1, 2\}) = \{\{1\}, \{2\}, \emptyset, \{1, 2\}\}$

(b) $\mathcal{P}(\{x, y, z\}) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{y, z\}, \{z, x\}, \{x, y, z\}\}$

Example 4.2.9

(a) $\mathcal{P}(\{1\}) = \{\{1\}, \emptyset\}$

(b) $\mathcal{P}(\mathcal{P}(\{1\})) = \{\emptyset, \{\{1\}\}, \{\{\emptyset, \{1\}\}\}, \{\emptyset\}\}$

(c) $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
$\mathcal{P}(\emptyset) = \{\emptyset\}$
$\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

Theorem 4.2.10

Let A be a set with $|A| = n$. Then $|\mathcal{P}(A)| = 2^n$

Proof: Let A be given so that $|A| = n$, encode the subsets of A with binary strings of length n. By the rule of product there are 2^n binary strings of length n.

Theorem 4.2.11

Show if $A \subseteq B$, then $\mathcal{P}(A) \subseteq \mathcal{P}(B)$

Proof: Suppose $A \subseteq B$ to show $\mathcal{P}(A) \subseteq \mathcal{P}(B)$

$$\text{Let } x \in \mathcal{P}(A)$$

$$\Rightarrow x \subseteq A$$

$$\Rightarrow x \subseteq B$$

$$\therefore x \in \mathcal{P}(B)$$