

COSC 311/317 COURSE WORKBOOK FALL 2023

EDITED BY PROFESSOR M.W. BERRY

Created by G. Ball'Khalsa, T. Beard, C. Edwards, P. Provins, S. Stoll, and D. Williams

*Department of Electrical Engineering and Computer Science
University of Tennessee, Knoxville*

August 24th, 2023 – December 5th, 2023

CONTENTS

1	Introduction to Sets: Notation and Operations	3
2	Combinatorics	9
2.1	The Rule of Sum	9
2.2	The Rule of Products	10
2.3	Permutations	11
2.4	Combinations	15
2.5	Summation Properties	18
2.6	Binomial Theorem	21
2.7	Combinations with Repetition	21
3	Logic and Proof Strategies	25
3.1	Propositions and Logical Operators	25
3.2	Truth Tables	27
3.3	Logical Equivalence	31
3.4	The Laws of Logic	34
3.5	Valid Arguments and the Rules of Inference	36
3.6	Propositions on a Set and Quantifiers	42
3.7	Rules for Theorem Proving	45
4	Set Theory	49
4.1	Set Operations and Laws	52
4.2	Laws of Set Theory	53
5	Mathematical Induction and Recursion	56
5.1	The Principle of Mathematical Induction	56
5.2	Recursive Definitions	65

6	Integer Properties	67
6.1	Division Algorithm	67
6.2	Greatest Common Division (Euclidean Algorithm)	71
6.3	RSA Encryption	74
7	Functions and Relations	78
7.1	Cartesian Products and Relations	78
7.2	Functions	79
7.3	Onto Functions	83
7.4	Function Composition and Inverse Functions	85
7.5	Computational Complexity	91
8	Graph Theory	98
8.1	Introduction	98
8.2	Subgraphs	105
8.3	Vertex Degree	113
8.4	Hypercube Architecture	114
8.5	Famous Problems	115
8.6	Planar Graphs	119
8.7	Bipartite Graphs	120
8.8	Elementary Subdivision and Homeomorphic Graphs	121
8.9	Euler's Theorem	125
9	Hamiltonian Paths and cycles	130
9.1	Definitions	130
9.2	Properties	131
9.3	Tournament Graphs	133
9.4	Useful Theorems and their Corollaries	135
9.5	Graph Coloring	135
10	Data Clustering Using Graphs	143
11	PageRank Algorithm for Importance Ranking	146
11.1	Normalized Importance	146
11.2	Random Jumps	147
11.3	PageRank	147

1 INTRODUCTION TO SETS: NOTATION AND OPERATIONS

Definition: A collection of objects is a set. The objects in a set are elements. Sets can be denoted by symbols or by using a set of curly braces where multiple elements listed inside are separated by commas.

Example 1: The set containing the integers 1, 2, and -10 is denoted as $\{1, 2, -10\}$. The following is also a set: $\{cat, 3, x, \square\}$. The integers form a set. A set with no elements is still a set, known as the empty set. A set can contain other sets such as $\{\{1\}, \{1, 2\}, \{2\}\}$.

Next, several commonly used sets, set notation, and some set operations are provided.

Notation for commonly used sets

- \mathbb{N} - the natural numbers, $\{0, 1, 2, 3, \dots\}$
- \mathbb{Z} - the integers, $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- \mathbb{Q} - the rational numbers
- \mathbb{R} - the real numbers
- \mathbb{C} - the complex numbers
- \emptyset - the set containing no elements, the empty set

Set notation and operations: (Assume A and B are sets.)

- $x \in A$ - the element x is in the set A
- $x \notin A$ - the element x is NOT in the set A
- $|A|$ - the cardinality of set A ; i.e. how many elements are in a set
- $A = B$ - The set A contains exactly the same elements as the set B and vice versa
- $A \subseteq B$ - the set A is a subset of set B and may be equal to the set B

- $A \subset B$ - the set A is a proper subset of set B but cannot be equal to the set B
- $A \cap B$ - the set formed from the *intersection* of sets A and B which are elements found in both sets **A AND B**.
- $A \cup B$ - the set formed from the *union* of sets A and B which are elements in sets **A OR B**. Here, OR is 'inclusive,' meaning elements in the union can be in *both* sets.
- A^c or \bar{A} - The set formed from the converse (or complement) of the set A (i.e. **NOT A**, elements not found in A .)
- $(A - B)$ - read as "A minus B" the set formed by the elements that are only in set A
- $A \oplus B$ - the elements in sets A and B , but not in both A and B (also denoted as **A XOR B**)

Example 2: The following set notation is read as *the set of all elements x in the integers such that x is greater than or equal to 0 and less than 4:*

$$\{x \in \mathbb{Z} | 0 \leq x < 4\}$$

and is equivalent to the set given by the following notation:

$$\{0, 1, 2, 3\}$$

Definition: Given a set A , the Power Set of A is the set containing every subset of the set A , and is denoted by $\mathcal{P}(A)$. (Note that \emptyset is a subset of A and therefore an element of $\mathcal{P}(A)$.)

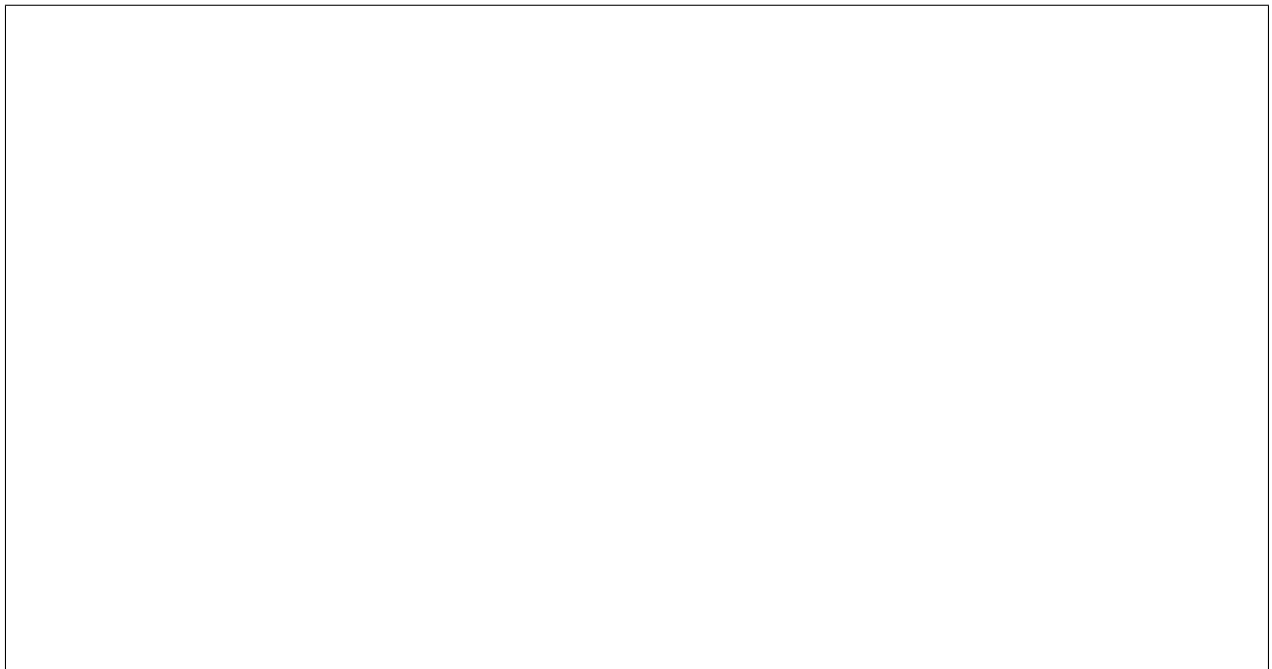
Definition: The Cartesian/Cross Product of two sets A and B , denoted $A \times B$, is the set

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Definition: A Universe of Discourse (or simply Universe) is the entire set of objects within which we are working for a particular context. It is usually denoted as, U . For example, the set of integers can be defined as the

universe of discourse, $U = \mathbb{Z}$, for a particular problem and then all other objects that are not integers would be excluded from the discussion or discourse that follows.

Definition: A Venn Diagram is a graphical construct of a universe of discourse in which a particular set is visualized using 1-3 usually overlapping circles each representing an individual set. For instance, let the rectangular box below represent some universe of discourse in which we will represent the sets A , B , and C as overlapping circles:



In Chapter 4, to facilitate working with more complicated statements involving sets, we will be more mathematically precise about some of the definitions presented here; however, the following exercises are intended to give you practice with the basic concepts of these definitions.

Chapter 1 Problems

1. Let $A = \{0, 2, 3, 6\}$, $B = \{1, 2, 3\}$, $C = \{1, 5, 9\}$, $D = \{2, 6, 8, 9\}$, and $E = \{2, 2, 8\}$.

Determine the following:

(a) $A \cap C$

(b) $D \cap (B \cup A)$

(c) $E \setminus (C \cap D)$

2. Are the following statements true? Provide explanations for your decisions.

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

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

(c) $A - B = B - A$

(d) $A \oplus B = B \oplus A$

3. Let A, B, and C be any sets. Draw a Venn Diagram for the set $A \cup (B \cap C)$



4. Construct the power set of each the following sets.

(a) $A = \{1,2,5,9\}$

(b) $B = \{\{1,2\}, \{3,4\}, \{5,6\}\}$

5. Let $A = \{4,5,7\}$ and $B = \{6,7\}$. for each item, construct the set or find the quantity for each expression below.

(a) $A \times B$

(b) $B \times A$

(c) B^2

(d) $|A \times B|$

(e) $|B \times A|$

2 COMBINATORICS

This chapter gives an introduction to combinatorics, the study of counting! Combinatorics is essential to areas such as probability, coding, cryptography, and graph theory.

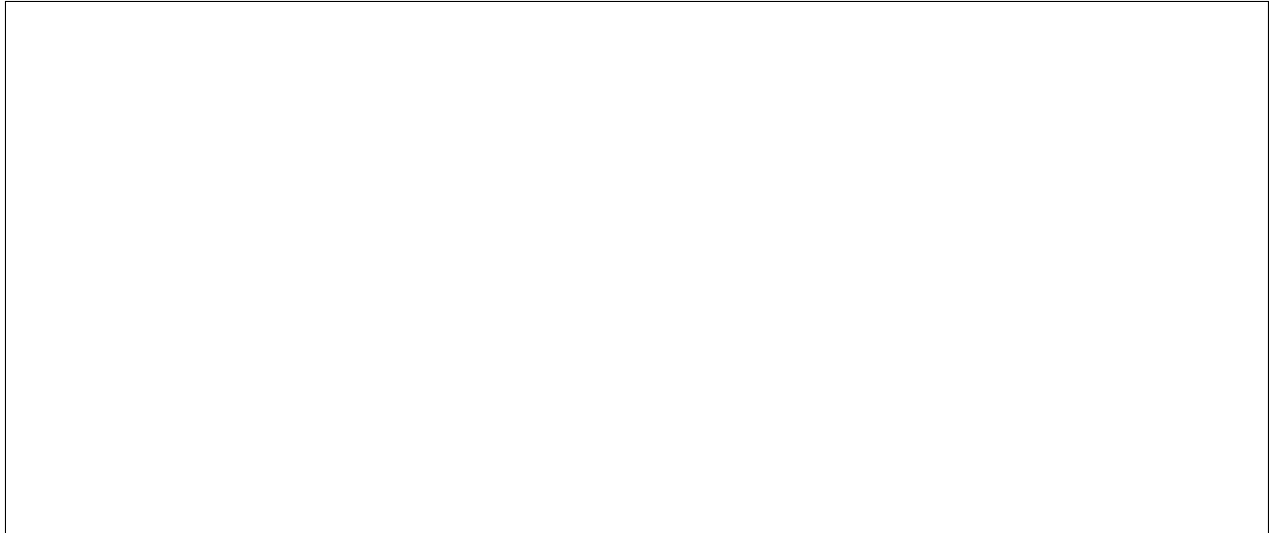
2.1 *The Rule of Sum*

- Task 1 can be done m distinct ways.
- Task 2 can be done n distinct ways.
- Assumption: Tasks cannot be done simultaneously so that either task can be done in one of $m + n$ ways.

Example 1: In Hodge's Library, there are 40 Sociology books available and 50 Anthropology books. How many books could Joe select from if he wants to learn about Sociology or Anthropology?

Answer: A student could select among $40 + 50 = 90$ books to learn about one or the other topic.

Example 2: Suppose a computer science instructor has seven different books each on the 3 programming languages: C++, Java, and Perl. Then, the instructor could recommend any one of twenty-one books to a student to learn concepts in programming. But now suppose that same instructor has two colleagues: one has three books on the analysis of algorithms and the other colleague has five books on the analysis of algorithms. Suppose n is the maximum number of different books on the topic of the analysis of algorithms that the instructor could borrow from them. What bounds can be imposed on n ?



2.2 *The Rule of Products*

The rule of products is used on problems which have two stages:

- Stage 1 has m possible outcomes.
- Stage 2 has n possible outcomes.
- You then *connect* every Stage 1 event to every Stage 2 event so that the total procedure can be carried out in $m \times n$ ways.

Example 1: A clothing manufacturer has put out a mix-and-match collection consisting of two blouses, two pairs of pants, a skirt, and a blazer. How many outfits can you make?

Answer: You can make $2 \text{ tops} \times 3 \text{ bottoms} \times 1 \text{ coat(s)} = 6$.

Example 2: Suppose license plates must have the form **AB1234**, that is, two letters followed by four integers (including zero).

- a. Assume no letter or digit can be repeated. How many different license plates can be printed?

- b. Now, allow repetitions of letters and digits. How many different license plates can be printed?

- c. Assuming repetitions, how many plates will have only vowels and even digits (zero is considered even)?

2.3 Permutations

A permutation of a set of objects is a particular linear arrangement of the objects. If there was a reshuffling of the objects (still arranged linearly) this would correspond to different permutations of the objects. Thus, when counting the possible number of permutations, we are concerned with counting how many different linear arrangements of objects there are and thus **order matters** with permutations.

Example 1: Suppose there are 10 students in a class and for a class photo we want to select five students for a particular row. How many arrangements are possible?

Answer:

$$\underbrace{10}_{1^{st}} \times \underbrace{9}_{2^{nd}} \times \underbrace{8}_{3^{rd}} \times \underbrace{7}_{4^{th}} \times \underbrace{6}_{5^{th}} = 30,240$$

More formally, we define permutation as follows:

Definition: Given n distinct objects, any linear arrangements of the n objects is called a permutation.

Permutations often involve the use of *factorials*, which are denoted with an exclamation point (!) and are defined as follows:

Factorial:

$$0! = 1$$

$$n! = n(n-1)(n-2) \cdots 3 \times 2 \times 1, \text{ for } n \geq 1$$

With this in place, we can see that given n distinct objects, the **number of permutations of size r for the n objects** is

$$P(n, r) = n \times (n-1) \times (n-2) \times \dots \times (n-r+1) = \frac{n!}{(n-r)!}$$

Example 2: Given the eight-letter word COMPUTER,

a) How many permutations of letters are possible?

$$\frac{8!}{(8-8)!} = 8!$$

b) How many 5 letter permutations are possible?

$$\frac{8!}{(8-5)!} = \frac{8!}{3!} = 6,720$$

c) Suppose repetitions are allowed and you allot sequences of 12 letters, how many permutations are possible?

$$8^{12} \simeq 6.872 \times 10^{10}$$

Permutations deal specifically with a set of *distinct* objects. However, we can consider linear arrangements of any set of objects even if some of the objects are the same as each other; i.e. there are objects in the set that are *indistinguishable* from one another. Thus, suppose we have n objects of which there are

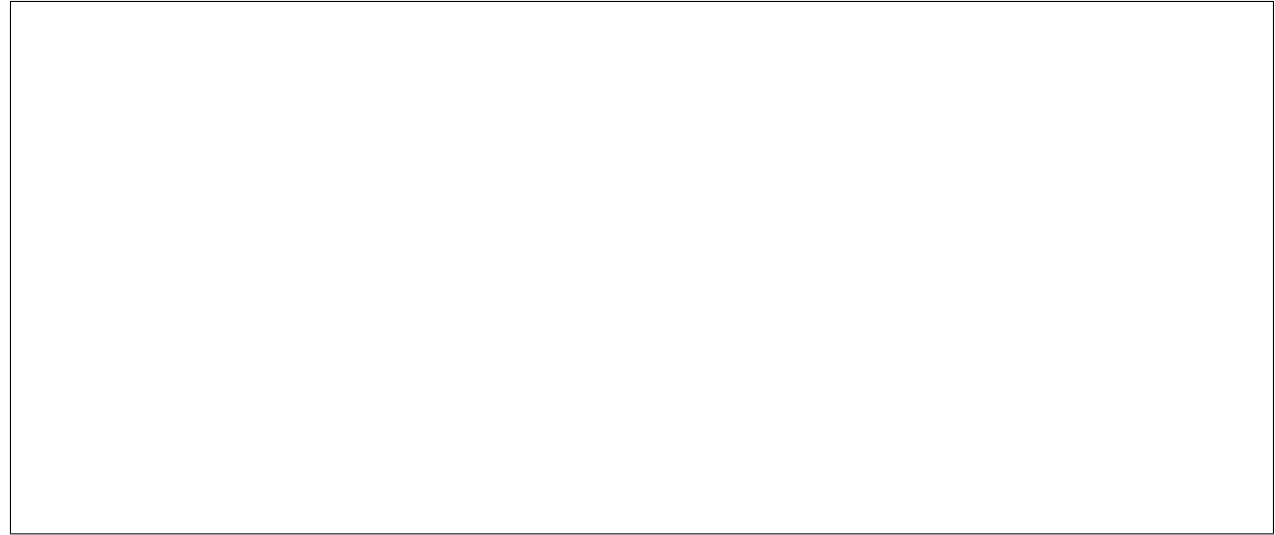
- n_1 indistinguishable objects of type 1,
- n_2 indistinguishable objects of type 2,
- \vdots
- n_r indistinguishable objects of type r ,

so that $n_1 + n_2 + \dots + n_r = \sum_{i=1}^r n_i = n$.

Then, there are $\frac{n!}{n_1! \times n_2! \times \dots \times n_r!}$ linear arrangements of the n objects.

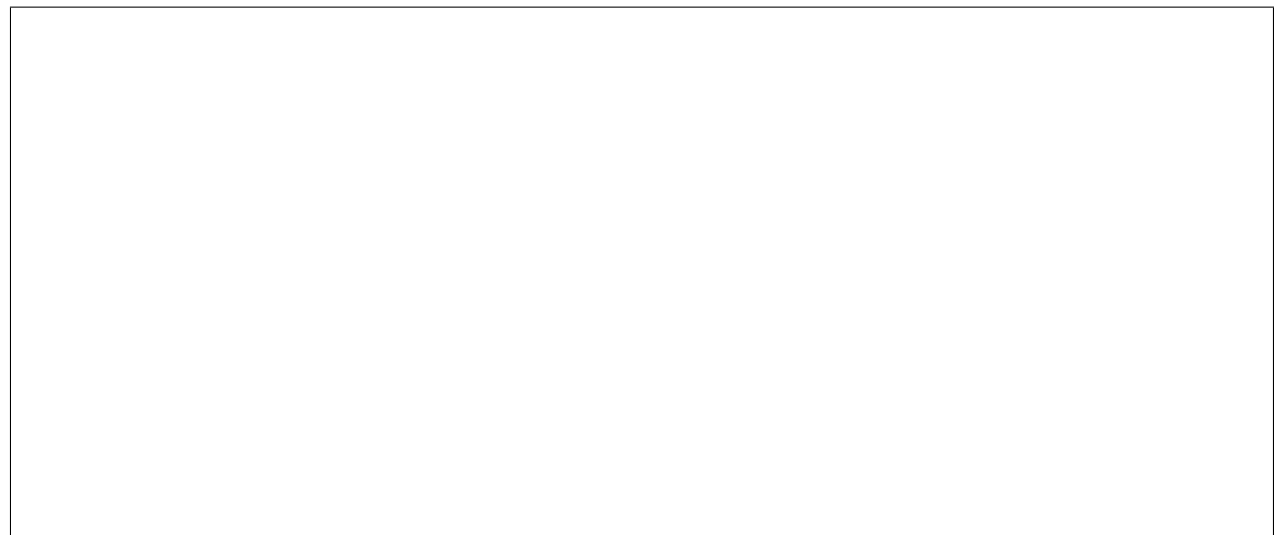
Example 3: How many unique permutations of letters in MISSISSIPPI can you create?

Example 4: Determine the number of staircase paths in the xy plane from the point $(2, 1)$ to the point $(7, 4)$ in which each path has individual steps going one unit to the right (R) or one unit up (U)? Hint: Every path will require 5 horizontal (R) moves and 3 vertical (U) moves. Why?



Nonlinear Arrangement

Example 5: Suppose there are six people $\{A,B,C,D,E,F\}$ seated around a circular table. How many different circular arrangements are possible if arrangements are considered the same if they differ only by a rotational shift?



Note that each circular arrangement corresponds to 6 distinct linear arrangements. These 6 arrangements are equivalent because without a beginning or end they all represent the same seating pattern.

A	B	C	D	E	F
B	C	D	E	F	A
C	D	E	F	A	B
D	E	F	A	B	C
E	F	A	B	C	D
F	A	B	C	D	E

So, $6 \times$ (number of circular arrangements of A,B,C,D,E,F)
 = number of linear arrangements of A,B,C,D,E,F = $6!$

Therefore, the number of circular arrangements of A,B,C,D,E,F = $\frac{6!}{6} = 120$.

2.4 Combinations

Unlike the situation with permutations, in some cases, a different ordering of n distinct objects does *not* constitute a different entity. For example, consider the following two situations:

- (a) 3 colors are to be selected from a given set of colors and each used to form a 3-striped flag;
- (b) 3 colors are to be selected to mix together into a new color.

For (a) above, one could make multiple distinct flags based on the ordering of the 3 colored stripes and so order matters, making this a permutation scenario. However, in (b) it does not matter the order in which the 3 colors were chosen; so the number of ways to select the 3 colors in (b) does not depend on the order in which they were chosen. This latter situation requires something related to a permutation but for which order does *not* distinguish different selections and this is where *combinations* come in.

Aside: don't be confused by the use of the word combination used in this context with the use for instance, regarding a locker combination... a locker combo is actually a permutation because the ordering of the numbers in the combo matters!

Definition: Given n distinct objects, each selection of r of these objects *without regard to order* corresponds to $r!$ permutations of size r from n objects. Thus, the number of combinations of r objects selected from n distinct objects without regard to order is defined and denoted by

$$C(n, r) = \binom{n}{r} = \frac{P(n, r)}{r!} = \frac{n!}{r! \times (n - r)!}, \text{ for } 0 \leq r \leq n.$$

It is also common to say " n choose r " when referring to combinations, $C(n, r)$.

Note these basic facts about combinations:

- For all $n \geq 0$: $C(n, 0) = C(n, n) = 1$
- For $n \geq 1$, $C(n, 1) = C(n, n - 1) = n$.
- If $0 \leq n < r$, then $C(n, r) = \binom{n}{r} = 0$.

Example 1: A student is taking a history exam containing 10 essay questions of which they must answer 7. How many ways are there for the student to select 7 of the questions to answer if:

- a) no other requirements are specified on how the 7 questions are chosen. (note: order is **not** important)?


- b) the student must answer 3 questions from the first 5 questions and 4 from the last 5 questions?

c) at least 3 questions must be selected from the first 5 questions?



Example 2: Sometimes the same problem can be viewed in terms of arrangements or combinations. Suppose a gym teacher wants to create 4 volleyball teams of 9 girls from a freshmen class of 36 girls. How many ways can the teacher select the 4 teams say A,B,C,D?

Answer using **combinations** whereby you form the A team first by selecting 9 girls and then form the remaining teams in succession:



Answer using **arrangements** whereby you line the students up in order and distribute 9 A's, 9 B's, 9 C's, and 9 D's across the 36 positions:

2.5 Summation Properties

Important properties of summation:

a) indices can vary: $\sum_{i=3}^7 a_i = \sum_{j=3}^7 a_j$.

b) zero index effect: $\sum_{i=1}^4 i^2 = \sum_{k=0}^4 k^2$.

c) index shifts: $\sum_{i=11}^{100} i^3 = \sum_{j=12}^{101} (j-1)^3 = \sum_{k=10}^{99} (k+1)^3$.

d) scalar factors: $\sum_{i=7}^{10} 2i = 2 \sum_{i=7}^{10} i$.

e) repeated scalar: $\sum_{i=1}^5 a = 5a$.

Example 1:

$$\binom{5}{3} \binom{5}{4} + \binom{5}{4} \binom{5}{3} + \binom{5}{5} \binom{5}{2} = \sum_{i=3}^5 \binom{5}{i} \binom{5}{7-i} = \sum_{j=2}^4 \binom{5}{7-j} \binom{5}{j}$$

Example 2: Suppose we have an alphabet of only three characters: 0,1,2. Define the string x by $x = x_1x_2\cdots x_n$, where each x_i is either 0, 1, or 2. Now define the function wt by $wt(x) = x_1 + x_2 + \cdots + x_n$ so that $wt(12) = 3$, $wt(22) = 4$, and $wt(101) = 2$. Among the 3^{10} strings of length 10 suppose we want to determine the number of strings that have **even** weight. The problem can be broken down into 6 cases representing the non-overlapping ways to form strings having even weight. Assume zero is an even number:

Case 1: x has no 1's.

Case 2: x has exactly two 1's.

Case 3: x has exactly four 1's.

Case 4: x has exactly six 1's.

2. COMBINATORICS

Case 5: x has exactly eight 1's.

Case 6: x has exactly ten 1's.

Since each case is independent of the others, we use the rule of sum to find the total number of ways to form strings that have even weight.

2.6 Binomial Theorem

The Binomial Theorem: Given variables x and y and a positive integer n , the repeated product of the term $(x + y)$ with itself (i.e. $(x + y)^n$) can be expanded as the following sum:

$$\begin{aligned}(x + y)^n &= \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \binom{n}{2}x^2y^{n-2} + \dots \\ &\quad + \binom{n}{n-1}x^{n-1}y^1 + \binom{n}{n}x^ny^0 \\ &= \sum_{k=0}^n \binom{n}{k}x^ky^{n-k}.\end{aligned}$$

Corollary to the Binomial Theorem: Given a positive integer n ,

$$\begin{aligned}\text{a) } &\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = 2^n \\ \text{b) } &\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \dots + (-1)^n \binom{n}{n} = 0.\end{aligned}$$

Fun fact: For n, r with $0 \leq r \leq n$, $\binom{n}{r} = \binom{n}{n-r}$. That is, without regard to order, the number of ways to choose r objects from n (n choose r) is the same as the number of ways to choose the amount of objects remaining (i.e., $n - r$) from n objects (n choose $n - r$). This may be a helpful perspective in some problems.

2.7 Combinations with Repetition

Consider the scenario in which one wants to select r objects from n distinct objects without regard to order and with *repetition*. For example, let's assume we have a set A with n elements and we can select r objects from A , where each object can be selected more than once. For instance, the combinations of letters a, b, c, d taken three at a time with repetition are:

$aaa, aab, aac, aad, abb, abc, abd, acc, acd, add, bbb, bbc, bbd, bcc, bcd, bdd,$
 $ccc, ccd, cdd, ddd.$

Note: Two combinations with repetition are considered **identical** if they have the same elements repeated the same number of time, regardless of their order (e.g., aab and baa).

Combinations with Repetition The number of combinations of r objects chosen from n distinct objects *with repetition*. is defined as:

$$\boxed{C(n + r - 1, r)}$$

Fun Fact: The number of combinations of n objects taken r at a time with repetition is equivalent to the number of ways r identical objects can be distributed among n distinct containers.

Example 1: Using the fun fact directly above, suppose you have $n = 3$ different (empty) milk containers and $r = 7$ quarts of milk that we can measure with a one quart measuring cup. In how many ways can we distribute the milk among the three containers?

To answer this question, let x_1, x_2, x_3 be the quarts of milk to put in containers 1, 2, and 3, respectively. The number of possible distributions of milk equals the number of non-negative integer solutions to $x_1 + x_2 + x_3 = 7$. Suppose we now use strokes or tick marks to represent a solution such as $x_1 = 2, x_2 = 1,$ and $x_3 = 4$. That is, $2 + 1 + 4$ is represented by $|| + | + ||||$. Hence, each possible solution could be thought of as an arrangement of $r = 7$ strokes and $(n - 1) = 2$ plus signs. So, the number of possible arrangements of the 9 symbols of which there are two types is given by

$$9! / (7! \times 2!) = \binom{9}{7}.$$

For any (n, r) pair, the resulting formula for counting combinations with

repetitions is given by

$$\binom{n+r-1}{r} = \frac{(n+r-1)!}{r!(n-1)!}.$$

Example 2: Suppose a message has 12 different symbols. In addition to 12 symbols, the transmitter also sends a total of 45 blank spaces between the symbols, with at least 3 spaces between each pair of executable symbols.

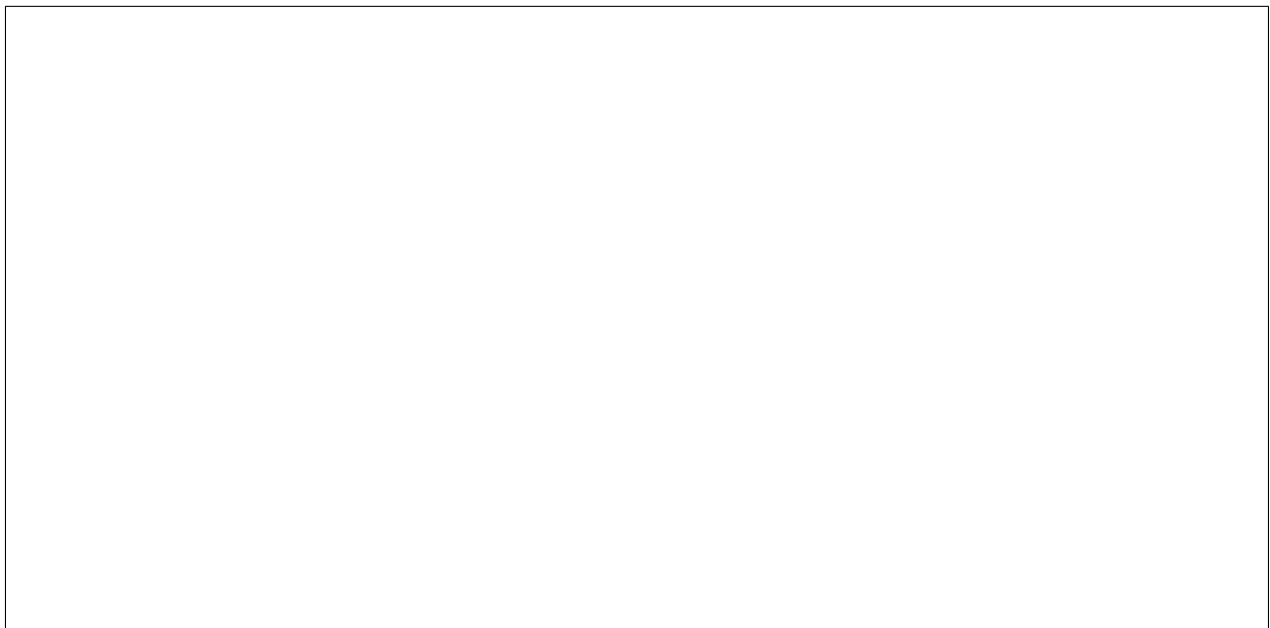
Question: How many ways can the transmitter send a message?

Answer: For 12 different symbols there are 12! different arrangements and for each arrangement there are 11 positions between the 12 symbols.

Let's illustrate this below:



There are 3 spaces between consecutive pairs, so 33 of the 45 spaces are automatically used to construct the message. This leaves 12 spaces to distribute (i.e., we have a selection problem). For 11 positions, we need to select 12 spaces to insert.



Example 3: Consider the following C++ code fragment below:

```
for (i=0; i < 20; i++) {  
    for (j=0; j <= i; j++) {  
        for (k=0; k <= j; k++) {  
            cout << i*j+k; }  
        }  
    }
```

Question: How many times is the cout statement executed?

Example 4: Consider the following C++ code fragment below:

```
count=0;  
for (i=0; i < n; i++) {  
    for (j=0; j <= i; j++) {  
        count++; }  
    }
```

Question: How many times is the count++; statement executed?

3 LOGIC AND PROOF STRATEGIES

3.1 Propositions and Logical Operators

Definition (Proposition/Statement): A **proposition** or **statement** is a declarative sentence (i.e., subject/verb/object) that is exclusively either true or false (not both). We say that a proposition *evaluates to either true or false* or *has a truth value of true or false*. (Note: A proposition can be a statement of opinion but not a command or question.)

Are the following sentences propositions? If they are, state their truth value. If they are not, explain why not.

1. Two plus five equals seven.
2. Two plus one equals eight.
3. No woman has ever been The Pope.
4. She is a defense lawyer.
5. That music is loud!
6. This proposition is false.
7. $x^3 - 5y = 0$
8. $A \cap B$

We often denote propositions with letters such as $p := "2 + 5 = 7"$ and $q := "5 > 7"$. *Simple or primitive propositions* such as these (i.e., one subject/one verb/one object) can be used to form *compound propositions* by utilizing the words/phrases *and*, *or* (inclusive), *exclusive or*, *not*, *if ... then ...*, and *... if and only if ...* to combine several primitive propositions into a single more complicated proposition. These connector words are called **logical connectives** and are denoted with symbols.

Let p and q be propositions. The following are new compound propositions comprised of p and q using logical connectives as illustrated below and followed by descriptive definitions of each:

$\neg p$	$p \wedge q$	$p \vee q$	$p \underline{\vee} q$	$p \rightarrow q$	$p \leftrightarrow q$
NOT	AND	OR	XOR	IMPLIES	IFF
“not p”	“p and q”	“p or q”	“p xor q”	“if p then q”	“p if and only if q”

Definition (NOT, NEGATION, \neg): The negation of a proposition p denoted $\neg p$ and read “not p ” is defined as a proposition that has the opposite truth value of p .

Definition (AND, \wedge): For two propositions p and q , the proposition formed as $p \wedge q$ is true only when both p is true and q is true; and false otherwise.

Definition (OR, \vee , inclusive): For two propositions p and q , the proposition formed as $p \vee q$ is true when p or q or both are true; and false otherwise. (i.e. it is only false when both p and q are false.)

Definition (XOR, Exclusive Or, $\underline{\vee}$): For two propositions p and q , the proposition formed as $p \underline{\vee} q$ is true when only one of p or q is true but *not* when both are true; and false otherwise.

Definition (implication, \rightarrow): For two propositions p and q , the proposition formed as $p \rightarrow q$ (“if p , then q .”) is only false when p evaluates as true but q evaluates false; but is true otherwise. It is also known as a *conditional proposition*, since the conclusion q is conditional on p . Note: the truth values of an implication based on the truth values of p and q are not the same as the validity or truth of the if-then claim itself as a proven or disproven argument.

Definition (if and only if, \leftrightarrow): For two propositions p and q , the proposition formed as $p \leftrightarrow q$ is defined as $p \rightarrow q$ and $q \rightarrow p$ (i.e. (if p then q) and (if q then p)). It is true only when both $p \rightarrow q$ and $q \rightarrow p$ evaluate to true. It is also known as a *biconditional proposition* and usually read as “ p if and only if q .”

Suppose we have the following (primitive) propositions $p :=$ "It's hot in Topeka." $q :=$ "It's sunny in Topeka." and $r :=$ "It's cloudy in Topeka."

1 Write out $\neg p$?

2 Write out $p \wedge q$?

3 Write out $p \vee q$?

4 Represent the following proposition with logical connectives: *If it's sunny in Topeka, then it's not cloudy in Topeka.*

5 Represent the following proposition with logical connectives: *It's not over 100 F in Topeka if and only if it's not sunny but cloudy in Topeka.*

3.2 Truth Tables

Denote truth values as True = 1 and False = 0. We can determine the truth value of a compound proposition by examining it under various permutations of truth values for the individual propositions that comprise the more complex proposition.

A *truth table* is a compact way to display the possible permutations of truth values, 0 and 1, for n individual statements in rows of the table.

Example 1: A truth table is illustrated below for $n = 2$ individual propositions p and q , to examine the compound propositions $\neg p$ and $p \vee q$:

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

Below is a truth table displaying the truth values for propositions, p and q , joined by the logical connectives:

p	q	$p \wedge q$	$p \vee q$	$p \underline{\vee} q$	$p \rightarrow q$	$p \leftrightarrow q$
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Example 2: (Simple Truth Table): Suppose p and q are propositions defined as follows: p : The old granola is bland. q : The fresh fruit is exquisite.

How could we make the proposition $p \vee q$ and how would it's truth table be filled out?

Example 3: (More Complex Truth Table): Suppose p , q and r are propositions defined as follows:

p : Combinatorics is a required course for Sophomores.

q : Margaret Mitchell wrote *Gone With the Wind*. r : $2 + 3 = 5$.

Let's generate a truth table for the above components and the compound statement:

“Margaret Mitchell wrote *Gone With the Wind* and if $2 + 3 \neq 5$, then combinatorics is a required class for sophomores.”



Definition (Tautology): A compound proposition is referred to as a *Tautology* if it is *true* for all truth value assignments.

Definition (Contradiction): A compound proposition is referred to as a *Contradiction* if it is *false* for all truth value assignments.

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$	T_0 “Tautology”	F_0 “Contradiction”
0	1	1	0	1	0
1	0	1	0	1	0

Definition (Contrapositive): The *contrapositive* of an implication $p \rightarrow q$ is defined as the implication proposition $\neg q \rightarrow \neg p$. (This will be shown later to be equivalent to the original implication!)

Definition (Converse): The *converse* of an implication $p \rightarrow q$ is defined as the implication $q \rightarrow p$.

Definition (Inverse): The *inverse* of an implication $p \rightarrow q$ is defined as the implication $\neg p \rightarrow \neg q$.

Example 4: Given propositions p and q , generate the truth values in the following table for $(p \vee q) \vee (\neg p)$ as well as $(p \wedge q) \wedge (\neg p)$. Hint: Form intermediate steps within the table for simpler propositions that comprise the original more complex proposition.

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

What can be said about the statement $(p \vee q) \vee (\neg p)$?

What can be said about the statement $(p \wedge q) \wedge (\neg p)$?

Example 5: Create a truth table for $[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$

p	q	r	$p \rightarrow (q \rightarrow r)$	$(p \rightarrow q) \rightarrow (p \rightarrow r)$	$[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$
0	0	0			
0	0	1			
0	1	0			
0	1	1			
1	0	0			
1	0	1			
1	1	0			
1	1	1			

What can be said about $[p \rightarrow (q \rightarrow r)] \rightarrow [(p \rightarrow q) \rightarrow (p \rightarrow r)]$?

3.3 Logical Equivalence

Definition (Logical Implication): If S_1 and S_2 are statements such that $S_1 \rightarrow S_2$ is a tautology, then we say that S_1 **logically implies** S_2 and write $S_1 \Rightarrow S_2$.

Definition (Logical Equivalence): Statements S_1 and S_2 are defined as **logically equivalent** when $S_1 \leftrightarrow S_2$ is a tautology. Logically equivalent statements, S_1 and S_2 , are denoted as $S_1 \Leftrightarrow S_2$.

Note: $(S_1 \Rightarrow S_2) \wedge (S_2 \Rightarrow S_1)$ is the same as $S_1 \Leftrightarrow S_2$. Logical equivalence is also bi-directional, this means that $(S_1 \Leftrightarrow S_2) \Leftrightarrow (S_2 \Leftrightarrow S_1)$.

Truth Tables and Logical Equivalence Logically equivalent statements are considered to be interchangeable and thus, *have identical truth values*.

Example 1: For statements p and q , show that $\neg p \vee q$ is logically equivalent to $p \rightarrow q$ using a truth table.

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

Some other properties of logical equivalences/implications:

1. If $p \Leftrightarrow q$, then $p \leftrightarrow q$ is a tautology and $p \rightarrow q$ and $q \rightarrow p$ are also tautologies.
2. If $p \not\Rightarrow q$, then $p \rightarrow q$ is not a tautology.

Definition (Dual): If S is a statement with no operations other than negation, \vee and \wedge , then the **dual** of S (S^d) is a statement obtained from S by replacing \wedge with \vee and vice-versa.

For example, if S is $(p \wedge \neg q) \vee (r \wedge T_0)$, then S^d is _____.

Theorem (Principle of Duality): Assume S and T are statements with no other operations other than negation (\neg), \wedge and \vee . If $S \Leftrightarrow T$ then $S^d \Leftrightarrow T^d$.

Substitution Rules:

1. Suppose P is in compound statement that is also a tautology. If p is a primitive statement that appears in *big* P and we replace every occurrence of p by another statement q , the resulting compound statement (P_1) is also a tautology.
2. Suppose P is a compound statement and little p is a statement appearing in P . Let q be a statement such $q \Leftrightarrow p$. If we replace one or more occurrences of p by q , then the resulting compound statement P_1 is logically equivalent to P , i.e., $P_1 \Leftrightarrow P$.

Example 2: Apply the first rule above to the following compound statement:

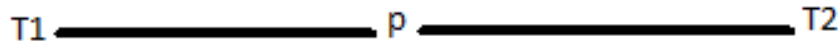
$$P : \neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q) ,$$

and note that P is a tautology. Replace p by $(r \wedge s)$ for all occurrences of little p to obtain a new tautology P_1 .

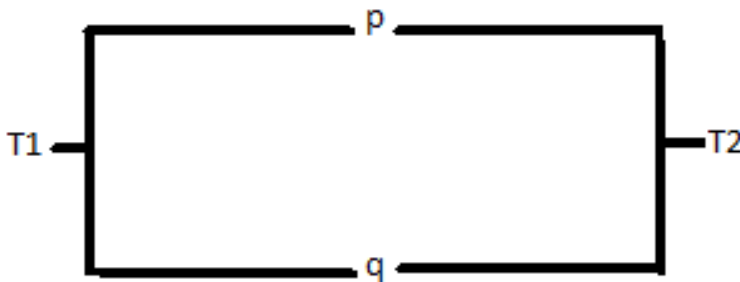
Example 3: For an application of the second (substitution) rule, suppose $P := (p \rightarrow q) \Leftrightarrow r$ and let $\hat{p} := p \rightarrow q$. Now suppose $\hat{p} \Leftrightarrow \hat{q}$ and we define $P_1 := \hat{q} \leftrightarrow r$. Can we conclude that $P_1 \Leftrightarrow P$? _____

Example 4: Consider a switching network of wires and switches connecting two terminals T_1 and T_2 . Assume when a switch is open (0), i.e., there is no current flow through it. Similarly when a switch is closed (1), there is current flow through it. Below are common switch topologies used in practice:

a. A simple switch:



b. Two switches in parallel ($p \vee q$):

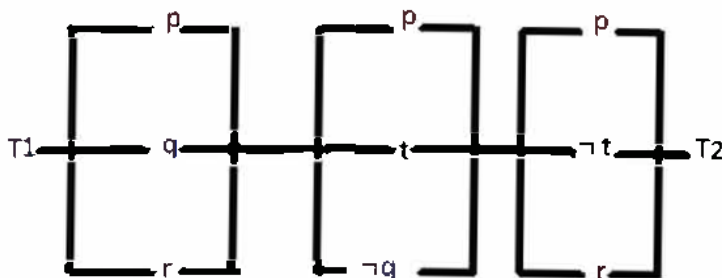


c. Two switches in series ($p \wedge q$):

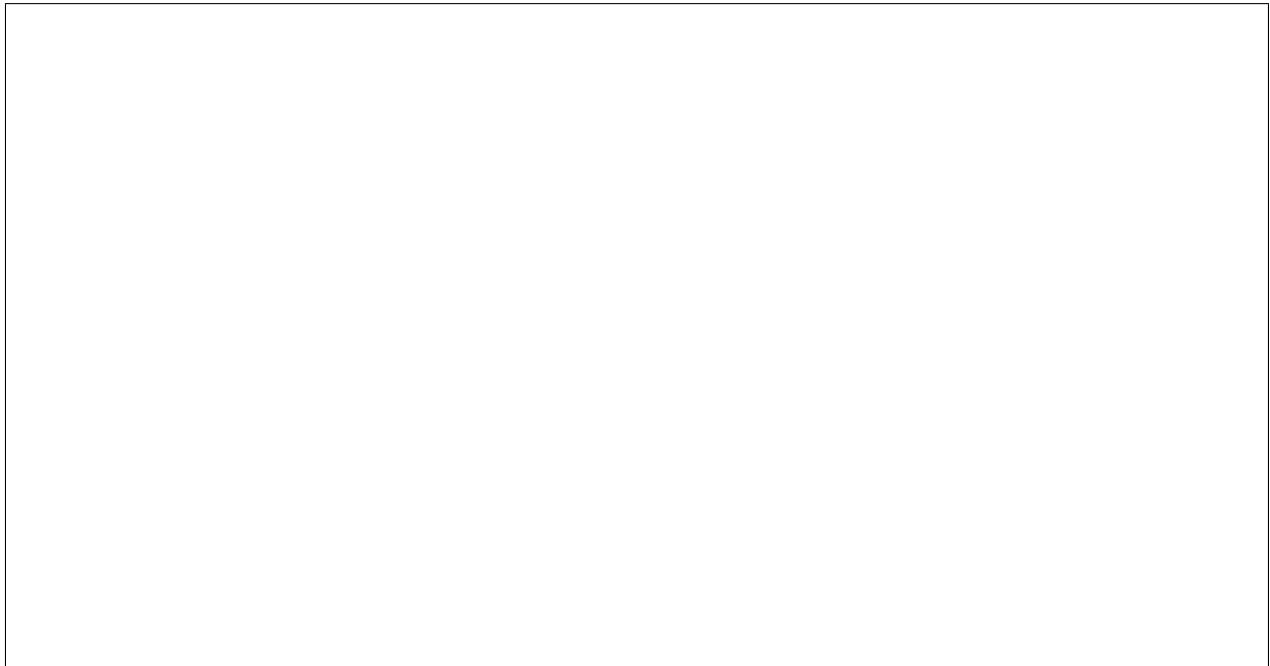
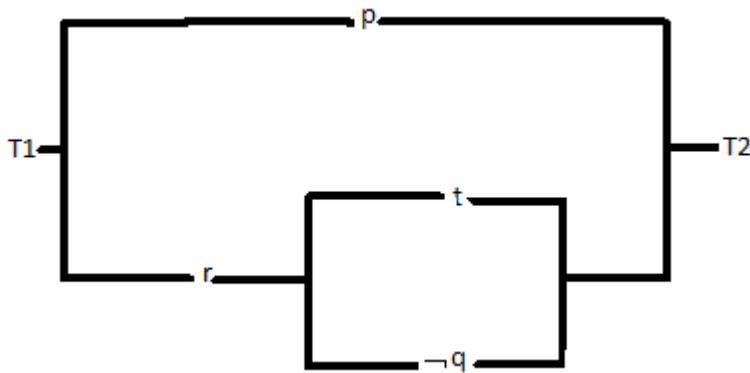


Example 5: Going off of the previous example, create a logic statement for the 9-switch network in (a) below and use our laws of logic to deduce that it is (logically) equivalent to the 4-switch network shown in (b).

a. Nine switches:



b. Four switches



3.4 *The Laws of Logic*

Certain logical implications and equivalences show up quite often and are now introduced as the "Laws of Logic" and "Rules of Inference."

Laws of Logic. Let p , q , and r be primitive (not compound) propositions and denote a tautology by T_0 and a contradiction by F_0 . The following are important **Laws of Logic**. Think about how you would prove that these laws are true for all p , q , and r .

a. Double Negation (Involution):

$$\neg(\neg)p \Leftrightarrow \underline{\hspace{2cm}}$$

b. DeMorgan's Laws:

$$\neg(p \vee q) \Leftrightarrow \underline{\hspace{2cm}}$$

$$\neg(p \wedge q) \Leftrightarrow \underline{\hspace{2cm}}$$

c. Commutative Laws:

$$p \vee q \Leftrightarrow \underline{\hspace{2cm}}$$

$$q \wedge p \Leftrightarrow \underline{\hspace{2cm}}$$

d. Associative Laws:

$$p \vee (q \vee r) \Leftrightarrow \underline{\hspace{2cm}}$$

$$p \wedge (q \wedge r) \Leftrightarrow \underline{\hspace{2cm}}$$

e. Distributive Laws:

$$p \vee (q \wedge r) \Leftrightarrow \underline{\hspace{3cm}}$$

$$p \wedge (q \vee r) \Leftrightarrow \underline{\hspace{3cm}}$$

f. Idempotent Laws:

$$p \vee p \Leftrightarrow \underline{\hspace{2cm}}$$

$$p \wedge p \Leftrightarrow \underline{\hspace{2cm}}$$

g. Identity Law:

$$p \vee (F_0) \Leftrightarrow \underline{\hspace{2cm}}$$

$$p \wedge (T_0) \Leftrightarrow \underline{\hspace{2cm}}$$

h. Inverse Laws:

$$p \vee \neg p \Leftrightarrow \underline{\hspace{2cm}}$$

$$p \wedge \neg p \Leftrightarrow \underline{\hspace{2cm}}$$

i. Domination Laws:

$$p \vee (T_0) \Leftrightarrow \underline{\hspace{2cm}}$$

$$p \wedge (F_0) \Leftrightarrow \underline{\hspace{2cm}}$$

j. Absorption Laws:

$$p \vee (p \wedge q) \Leftrightarrow \underline{\hspace{2cm}}$$

$$p \wedge (p \vee q) \Leftrightarrow \underline{\hspace{2cm}}$$

k. Conditional Law:

$$p \rightarrow q \Leftrightarrow \underline{\hspace{2cm}}$$

l. Biconditional Equivalences:

$$(p \leftrightarrow q) \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p) \Leftrightarrow \underline{\hspace{2cm}} (\neg p \wedge \neg q)$$

m. Contrapositive:

$$(p \rightarrow q) \Leftrightarrow \underline{\hspace{2cm}}$$

3.5 Valid Arguments and the Rules of Inference

For the compound statement (assuming n is a positive integer)

$$(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \rightarrow q,$$

we call P_1, P_2, \dots, P_n the **premises** of the argument and q the **conclusion** of the argument.

Example 1: Suppose we have the following primitive statements:

p := "Roger studies"

q := "Roger plays raquetball"

r := "Roger passes COSC 311."

Consider the following three premises

P_1 : If Roger studies, he will pass the class. $(p \rightarrow r)$

P_2 : If Roger doesn't play raquetball, he will study. $(\neg q \rightarrow p)$

P_3 : Roger failed the class. $(\neg r)$

for the argument $(P_1 \wedge P_2 \wedge P_3) \rightarrow q$. Complete the truth table for the argument

$$[(p \rightarrow r) \wedge (\neg q \rightarrow p) \wedge \neg r] \rightarrow q,$$

and show that it is in fact a **tautology**.

p	q	r	$p \rightarrow r$	$\neg q \rightarrow p$	$\neg r$	q	$(P_1 \wedge P_2 \wedge P_3) \rightarrow q$
0	0	0					
0	0	1					
0	1	0					
0	1	1					
1	0	0					
1	0	1					
1	1	0					
1	1	1					

Rules of Inference Now we present some very common and useful valid arguments known as Rules of Inference.

1. Rule of Detachment:

$$(p \rightarrow q) \wedge p \Rightarrow \underline{\hspace{2cm}}$$

2. Law of Syllogism (Chain Rule):

$$(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow \underline{\hspace{3cm}}$$

3. Indirect Reasoning (Modus Tollens, The Method of Denying):

$$(p \rightarrow q) \wedge (\neg q) \Rightarrow \underline{\hspace{2cm}}$$

4. Disjunctive Amplification (or Addition):

$$p \Rightarrow \underline{\hspace{2cm}}$$

5. Conjunctive Simplification:

$$(p \wedge q) \Rightarrow \underline{\hspace{2cm}}$$

$$(p \wedge q) \Rightarrow \underline{\hspace{2cm}}$$

6. Disjunctive Simplification (or Disjunctive Syllogism):

$$(p \vee q) \wedge \neg p \Rightarrow \underline{\hspace{2cm}}$$

$$(p \vee q) \wedge \neg q \Rightarrow \underline{\hspace{2cm}}$$

7. Rule of Contradiction:

$$\neg p \rightarrow F_0 \Rightarrow p$$

Now we will look at some of these rules and show how to prove that they are **valid arguments** (i.e., implication statements that are tautologies). First note the following notation convention.

Recall that the **Law of Syllogism** is given by the tautology

$$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r) .$$

We can write the premises and conclusion of this implication using a tabular form:

$$\begin{array}{l} p \rightarrow q \quad \text{premise 1} \\ q \rightarrow r \quad \text{premise 2} \\ \hline \therefore p \rightarrow r \quad \text{conclusion} \end{array}$$

Example 2: Rules of Inference displayed in tabular form.

- a. The Indirect Reasoning tautology (or *The Method of Denying, Modus Tollens*) in tabular form is given by:

$$\begin{array}{l} p \rightarrow q \\ \neg q \\ \hline \therefore \neg p \end{array}$$

- b. The Rule of Disjunctive Syllogism tautology in tabular form is given by:

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Example 3: As seen above in the list of Inference Rules, the Rule of Detachment (or *Modus Ponens*) is given by

$$[p \wedge (p \rightarrow q)] \rightarrow q .$$

In tabular form we can write this tautology as

$$\begin{array}{l} p \quad \text{premise 1} \\ p \rightarrow q \quad \text{premise 2} \\ \hline \therefore q \quad \text{conclusion} \end{array}$$

Example 4: Let's use two approaches to prove that the following is a valid argument using the rules of inference and/or laws of logic:

$$\begin{array}{l}
 p \\
 p \rightarrow \neg q \\
 \neg q \rightarrow \neg r \\
 \hline
 \therefore \neg r
 \end{array}$$

Approach 1

Approach 2

<u>Step</u>	<u>Reason(s)</u>	<u>Step</u>	<u>Reason(s)</u>
1. _____	Premise	1. _____	Premise
2. _____	Premise	2. _____	Premise
3. _____	Law of Syllogism	3. _____	Rule of Detachment
4. _____	Premise	4. _____	Premise
5. _____	Rule of Detachment	5. _____	Rule of Detachment

Example 5: Prove that the following implication is a valid argument using the rules of inference and/or laws of logic. Provide reason(s) for each step in the proof.

$$\begin{array}{l}
 p \rightarrow q \\
 \neg q \\
 \neg r \\
 \hline
 \therefore \neg(p \vee r)
 \end{array}$$

Proof by Contradiction. The Rule of Conjunction given below together with the Rule of Contradiction are both tautologies having the respective tabular forms below. With these, we form the method of proof known as *Proof by Contradiction*. This is a very powerful and useful method, but it must be set up carefully!

Conjunction	Contradiction
$\frac{p}{q}$	$\frac{\neg p \rightarrow F_0}{}$
$\therefore p \wedge q$	$\therefore p$

Using the above rules of inference, a Proof by Contradiction (or *Reductio Absurdum*) to establish the tautology

$$(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \rightarrow q$$

is achieved by establishing the logically equivalent tautology:

$$(P_1 \wedge P_2 \wedge \cdots \wedge P_n \wedge \neg q) \rightarrow F_0$$

Example 6: Note that the method of proof by contradiction as outlined above is claiming that the following biconditional statement is a tautology:

$$(p \rightarrow q) \leftrightarrow [(p \wedge \neg q) \rightarrow F_0]$$

Let's verify the tautology using a truth table. Recall that \leftrightarrow means "if and only if."

Example 7: Let's take a look at an example where we will construct a logical argument and then prove that the argument is in fact a tautology. First, we will prove it directly, assuming the premises as usual and reasoning to the conclusion, p , *directly*. Then, we will prove it another way by using the method of a proof by contradiction. Which proof will you like best??

Suppose a band can play rock music (p) and refreshments can be delivered on time (q). But suppose a New Year's Eve party is cancelled (r) and the host Alicia is angry (s) and must make refunds to her guests (t). If the band does not play rock music or refreshments do not arrive on time ($\neg p \vee \neg q$), then the party has to be cancelled making Alicia angry ($r \wedge s$). Also, if the party is cancelled (r) then refunds have to be made to the guests (t). It turns out that refunds did not have to be made ($\neg t$), so we conclude that the band played rock music (p). In tabular form, the resulting argument can be expressed as:

$$\begin{array}{l} (\neg p \vee \neg q) \rightarrow (r \wedge s) \\ r \rightarrow t \\ \neg t \\ \hline \therefore p \end{array}$$

Let's complete the following proof that validates the argument above.

<u>Step</u>	<u>Reason(s)</u>
1. $r \rightarrow t$	Premise
2. $\neg t$	Premise
3. $\neg r$	Modus Tollens
4. _____	Disjunctive Addition
5. _____	DeMorgan's Law
6. $(\neg p \vee \neg q) \rightarrow (r \wedge s)$	Premise
7. _____	Modus Tollens
8. _____	DeMorgan's Law & Double Negation
9. $\therefore p$	Conjunctive Simplification

3.6 Propositions on a Set and Quantifiers

Definition (Open Proposition): An *open* proposition (i) has one or more variables belonging to a specified set of some universe, (ii) is not a proposition on its own, and (iii) becomes a proposition when the variables are replaced by values.

Example 1: Let $U = \mathbb{Z}$ and let $x \in \mathbb{Z}$. Consider the following open proposition

$$p(x) := \text{"The number } x + 2 \text{ is an even integer"}$$

Clearly, in the universe of integers $p(5) := \text{"The number 7 is an even integer."}$ is false; and $\neg p(7) := \text{"The number 7 is not an even integer."}$ is true.

We often use the following *quantifiers* and respective notation for open propositions, where U is some universe and $x \in U$:

- a. **Existential Quantifier**—"there exists x " or $\exists x$; also: "there exists $x \in U$ " or $\exists x \in U$;
- b. **Universal Quantifier**—"for all x " or $\forall x$; also: "for all $x \in U$ " or $\forall x \in U$.

Example 2: Suppose you have the following four open statements with $x \in \mathbb{R}$:

$$\begin{aligned} p(x): x \geq 0 & \quad r(x): x^2 - 3x - 4 = 0 \\ q(x): x^2 \geq 0 & \quad s(x): x^2 - 3 > 0 \end{aligned}$$

Mark each statement below as either true or false.

$$\begin{aligned} \exists x [p(x) \wedge r(x)] & \quad \underline{\hspace{2cm}} \\ \forall x [p(x) \rightarrow q(x)] & \quad \underline{\hspace{2cm}} \\ \forall x [q(x) \rightarrow s(x)] & \quad \underline{\hspace{2cm}} \\ \forall x [r(x) \vee s(x)] & \quad \underline{\hspace{2cm}} \\ \forall x [r(x) \rightarrow p(x)] & \quad \underline{\hspace{2cm}} \end{aligned}$$

Example 3: Now change the universe to \mathbb{Z} in Example 2 above and determine if your answers change.

Example 4: Consider the following C++ code statement below:

```
for (n=0; n < 20; n++) {A[n]=n*n-n;}
```

Assuming all elements of the array A are integers, determine whether each open statement below is true or false?

- $\forall n (A[n] \geq 0)$ _____
- $\exists n (A[n+1] = 2 * A[n])$ _____
- $\forall n [(0 \leq n < 20) \rightarrow (A[n] < A[n+1])]$ _____
- $\forall m \forall n [(m \neq n) \rightarrow (A[m] \neq A[n])]$ _____

Logical Equivalence versus Logical Implication for Open Propositions:

If $\forall x[p(x) \Leftrightarrow q(x)]$, then $p(a) \Leftrightarrow q(a)$ for all a in a given universe.

If $p(a) \rightarrow q(a)$ for every a in a given universe, then $\forall x[p(x) \Rightarrow q(x)]$.

Definition: Consider the quantified open proposition: $\forall x[p(x) \rightarrow q(x)]$, where $p(x)$ and $q(x)$ are open statements over some set in a universe, U .

1. The **contrapositive** of $\forall x[p(x) \rightarrow q(x)]$ is $\forall x[\neg q(x) \rightarrow \neg p(x)]$.
2. The **converse** of $\forall x[p(x) \rightarrow q(x)]$ is $\forall x[q(x) \rightarrow p(x)]$.
3. The **inverse** of $\forall x[p(x) \rightarrow q(x)]$ is $\forall x[\neg p(x) \rightarrow \neg q(x)]$.

Example 5: Suppose you have the following four open statements:

$$p(x): |x| > 3 \quad \neg p(x): |x| \leq 3$$

$$q(x): x > 3 \quad \neg q(x): x \leq 3$$

Mark each statement below as either true or false.

- $\forall x [p(x) \rightarrow q(x)]$ _____
- $\forall x [q(x) \rightarrow p(x)]$ _____ (converse)
- $\forall x [\neg p(x) \rightarrow \neg q(x)]$ _____ (inverse)
- $\forall x [\neg q(x) \rightarrow \neg p(x)]$ _____ (contrapositive)

Logical Implications and Equivalences for Open Statements (One Variable):

Assume $p(x)$ and $q(x)$ are open statements on the same prescribed universe of values. The following are important logical implications/equivalences involving quantifiers:

1. $\forall x p(x) \Rightarrow \exists x p(x)$
2. $\exists x [p(x) \wedge q(x)] \Rightarrow \exists x p(x) \wedge \exists x q(x)$
3. $\exists x [p(x) \vee q(x)] \Leftrightarrow [\exists x p(x) \vee \exists x q(x)]$
4. $\forall x [p(x) \wedge q(x)] \Leftrightarrow [\forall x p(x) \wedge \forall x q(x)]$
5. $\forall x p(x) \vee \forall x q(x) \Rightarrow \forall x [p(x) \vee q(x)]$

Negating Quantifiers: Assume $p(x)$ is an open statement on a prescribed universe of values. The following logical equivalences demonstrate how to correctly negate quantified open propositions.

1. $\neg [\forall x p(x)] \Leftrightarrow \exists x \neg p(x)$.
2. $\neg [\exists x p(x)] \Leftrightarrow \forall x \neg p(x)$.
3. $\neg [\forall x \neg p(x)] \Leftrightarrow \exists x p(x)$.
4. $\neg [\exists x \neg p(x)] \Leftrightarrow \forall x p(x)$.

Example 6: Consider the following five open statements over the universe of integers:

$$p(x): x > 0$$

$$q(x): x \text{ is even}$$

$$r(x): x \text{ is a perfect square}$$

$$s(x): x \text{ is exactly divisible by 4}$$

$$t(x): x \text{ is exactly divisible by 5}$$

Provide the symbolic forms for each of the following open statements with quantifiers:

- a. "At least one integer is even." _____
- b. "There exists a positive integer that is even." _____

- c. "If x is even, then x is not divisible by 5." _____
- d. "No even integer is divisible by 5." _____
- e. "There exists an even integer divisible by 5." _____
- f. "If x is even and x is a perfect square, then x is divisible by 4." _____

Example 7: Assuming the universe of real numbers, let's negate (and simplify) the following open statements:

- a. $\forall x \forall y [(x > y) \rightarrow (x - y > 0)]$ _____
- b. $\forall x \forall y [(x < y) \rightarrow \exists z (x < z < y)]$ _____
- c. $\forall x \forall y [(|x| = |y|) \rightarrow (y = \pm x)]$ _____

3.7 Rules for Theorem Proving

One way to prove a statement is true for all values in a given universe is to do so by brute force: test all possible values from the universe to show or determine which ones make the open statement true. Rightly so, this is referred to as the **Method of Exhaustion** and is typically not a feasible strategy. Thus, we consider two general rules to facilitate proving theorems that involve quantifiers on open statements. The first one we consider is the *Rule of Universal Specification*, a logical implication stated in the previous section and now discussed in more detail.

Rule of Universal Specification (or RUS):

If a particular open statement becomes true for all replacements by elements of a given universe, then the open statement is true for each specific individual element (value) in the universe. Symbolically, we write

If $\forall x p(x)$ is true, then $p(a)$ is true for each a in the universe.

Example 1: Suppose the universe consists of all people and let $m(x)$ return true if person x is a math professor and $c(x)$ return true if person x has studied calculus. Consider the following argument:

All math professors have studied calculus. Leona is a math professor.
Therefore, Leona has studied calculus.

We can use RUS to argue that Leona (person l) indeed studied calculus.

$$\begin{array}{ll} \forall x [m(x) \rightarrow c(x)] & \text{Premise} \\ m(l) & \text{Premise} \\ \hline \therefore c(l) & \text{RUS} \end{array}$$

Rule of Universal Generalization (or RUG):

If open statement $p(x)$ is proved to be true when x is replaced by any *arbitrarily chosen* element c from the universe, then $\forall x p(x)$ is true.

Example 2: Suppose $p(x)$, $q(x)$ and $r(x)$ are open statements on the same universe (of values). Prove the validity of the following argument:

$$\begin{array}{ll} \forall x [p(x) \rightarrow q(x)] & \text{Premise} \\ \forall x [q(x) \rightarrow r(x)] & \text{Premise} \\ \hline \therefore \forall x [p(x) \rightarrow r(x)] & \text{Conclusion} \end{array}$$

<u>Step</u>	<u>Reason(s)</u>
1. $\forall x [p(x) \rightarrow q(x)]$	Premise
2. $p(c) \rightarrow q(c)$	_____
3. $\forall x [q(x) \rightarrow r(x)]$	Premise
4. $q(c) \rightarrow r(c)$	_____
5. _____	Law of Syllogism
<hr/>	
6. $\therefore \forall x [p(x) \rightarrow r(x)]$	_____

Common proof strategies include

1. Direct Proof
2. Contrapositive Argument
3. Proof by Contradiction

Let's demonstrate each of these in the following examples where we will use the following definitions:

Definition: An integer $n \in \mathbb{Z}$ is **even** if there exists an integer $k \in \mathbb{Z}$ such that $n = 2k$. Zero is considered as an even integer.

Definition: An integer $n \in \mathbb{Z}$ is **odd** if there exists an integer $k \in \mathbb{Z}$ such that $n = 2k + 1$.

Example 3: (Direct Proof) For all integers k and l , if k and l are odd, then their product is also odd.

Proof. Since k and l are odd, we can write $k = 2a + 1$ and $l = 2b + 1$ for some integer a and b . Then, $kl = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$. Since $2ab + a + b$ is an integer, then kl must be odd. \square

Example 4: (Direct Proof) If m is an even integer, then $m + 7$ is odd.

Proof. Since m is even, we can write $m = 2a$, for some integer a . Then, $m + 7 = 2a + 7 = 2a + 6 + 1 = 2(a + 3) + 1$. Since $a + 3$ is an integer, $m + 7$ must be odd. \square

Example 5: (Contrapositive Argument) If m is an even integer, then $m + 7$ is odd.

Proof. Suppose $m + 7$ is not odd, hence even. Then, we can write $m + 7 = 2b$, for some integer b . So $m = 2b - 7 = 2b - 8 + 1 = 2(b - 4) + 1$ and $b - 4$ is an integer. But m would have to be odd contradicting the assumption that m is even. Therefore, $m + 7$ must be odd. \square

Example 6: (Proof by Contradiction) If m is an even integer, then $m + 7$ is odd.

Proof. Assume m is even and that $m + 7$ is also even. Then, we can write $m + 7 = 2c$, for some integer c . So, $m = 2c - 7 = 2(c - 4) + 1$ with $c - 4$ an integer. Hence, m must be odd and that contradicts our assumption that m is even. Therefore, $m + 7$ must be odd (not even). \square

4 SET THEORY

Definitions: Set Equality, Subset, and Proper Subset: Let C and D be sets from a universe U . Then,

- If for every $x \in C$, we also have $x \in D$ and in addition, if for every $x \in D$, we have $x \in C$, (i.e. the sets C and D contain exactly the same elements), then we say C and D are equal and denote this $C = D$.
- If for every $x \in C$, we also have $x \in D$, then we say that C is a subset of D and denote this as $C \subseteq D$.
- If for every $x \in C$, it is true that $x \in D$ and in addition there exists $y \in D$ such that $y \notin C$ (i.e D contains elements that are not also in C), then we say that C is a proper subset of D , denoted by $C \subset D$ (i.e. equality of the two sets is not possible.)

Notes:

- The use of \subseteq to describe set relationships includes the logical inclusive *or* option of a proper subset relationship *or* set equality.
- Using the definition of subset, it follows directly that if $C \subseteq D$ and $D \subseteq C$, then $C = D$.
- Note that $|\emptyset| = 0$ (i.e. the cardinality of the empty set is zero) and $\{0\} \neq \emptyset$ (i.e. the set containing the element zero is not equal to the empty set).

Example 1: Suppose we have the universe

$$U = \{1, 2, 3, 4, 5, 6, x, y, \{1, 2\}, \{1, 2, 3\}, \{1, 2, 3, 4\}\}$$

so that $|U| = 11$. If $A = \{1, 2, 3, 4\}$, is $A \in U$? _____. If $\{A\}$ is a set that only contains the set A , is $\{A\} \subset U$? _____. So, is there a difference between A as an element of the universe and $\{A\}$ as a subset of the universe? _____. Is $\{A\} \notin U$ true? _____

Example 2: Suppose the universe $U = \{1, 2, 3, 4, 5\}$ and $A = \{1, 2, 3\}$, $B = \{3, 4\}$, and $C = \{1, 2, 3, 4\}$. Determine the validity of the following statements:

$$\begin{array}{ll} A \subset C & \underline{\hspace{2cm}} \quad B \subset C \quad \underline{\hspace{2cm}} \\ B \not\subset A & \underline{\hspace{2cm}} \quad A \not\subset A \quad \underline{\hspace{2cm}} \\ A \subset A & \underline{\hspace{2cm}} \quad B \not\subset A \quad \underline{\hspace{2cm}} \end{array}$$

Example 3: Recall from Section 1 that the **power set** of a set A , denoted by $\mathcal{P}(A)$, is the set of all possible subsets of the set A . Suppose $C = \{1, 2, 3, 4\}$. Derive $\mathcal{P}(C)$ and $|\mathcal{P}(C)|$.

Below are logically equivalent statements involving subsets and set equality:

Logical Equivalences for Subsets:

$$\begin{aligned} A \subseteq B &\Leftrightarrow \forall x [x \in A \Rightarrow x \in B] \\ A \not\subseteq B &\Leftrightarrow \neg \forall x [x \in A \Rightarrow x \in B] \\ &\Leftrightarrow \exists x \neg [x \in A \Rightarrow x \in B] \\ &\Leftrightarrow \exists x \neg [\neg(x \in A) \vee x \in B] \\ &\Leftrightarrow \exists x [x \in A \wedge \neg(x \in B)] \\ &\Leftrightarrow \exists x [x \in A \wedge x \notin B] \\ A = B &\Leftrightarrow A \subseteq B \wedge B \subseteq A \\ A \neq B &\Leftrightarrow \neg [A \subseteq B \wedge B \subseteq A] \\ &\Leftrightarrow \neg (A \subseteq B) \vee \neg (B \subseteq A) \\ &\Leftrightarrow (A \not\subseteq B) \vee (B \not\subseteq A) \\ A \subset B &\Leftrightarrow (A \subseteq B) \wedge (A \neq B) \end{aligned}$$

Theorem (Dimension of Power Set): If the set A is finite and $|A| = n$, where $n \geq 0$. Then, A has 2^n subsets, or $|\mathcal{P}(A)| = 2^n$.

Proof.

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = \sum_{k=0}^n \binom{n}{k} = 2^n, \text{ for } n \geq 0.$$

□

Example 4: Let's revisit the staircase path problem and consider a path on the xy grid from the point $(2,1)$ to the point $(7,4)$. Let U denote a move upward and R denote a move to the right. Two possible paths are illustrated below as subsets of upward moves:

1	2	3	4	5	6	7	8	U subset
R	U	R	R	U	R	R	U	$\{2,5,8\}$
U	R	R	R	U	U	R	R	$\{1,5,6\}$

How many ways can we choose 3 upward moves or how many ways can we choose 5 moves to the right?

Special Sets:

- \mathbb{Z} = integers $\{0, 1, -1, 2, -2, \dots\}$
- \mathbb{N} = nonnegative integers $\{0, 1, 2, 3, \dots\}$ (natural numbers)
- \mathbb{Z}^+ = positive integers $\{1, 2, 3, \dots\}$ or $\{x \in \mathbb{Z} | x > 0\}$
- \mathbb{Q} = rational numbers $\{a/b \mid a, b \in \mathbb{Z} \wedge b \neq 0\}$
- \mathbb{Q}^+ = positive rational numbers $\{r \in \mathbb{Q} \wedge r > 0\}$
- \mathbb{R} = real numbers

4.1 Set Operations and Laws

Let A and B be two subsets of the universe U . Then,

- $A \cup B$ is the **union** of A and B defined by $\{x | x \in A \vee x \in B\}$.
- $A \cap B$ is the **intersection** of A and B defined by $\{x | x \in A \wedge x \in B\}$.
- $A \Delta B$ is the **symmetric difference** of A and B defined by $\{x | (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B)\} = \{x | x \in (A \cup B) \wedge x \notin (A \cap B)\}$.

Example 1: Suppose $U = \{1, 2, 3, \dots, 10\}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 5, 6, 7\}$, and $C = \{7, 8, 9\}$. Determine $A \Delta B$ and $A \Delta C$.

Definition (Disjointness): If $S, T \subseteq U$, then S and T are **disjoint** (or mutually disjoint) if $S \cap T = \emptyset$.

Theorem: For $S, T \subseteq U$, S and T are disjoint if and only if $S \cup T = S \Delta T$.

Definition (Complement): For $A \subseteq U$, the **complement** of A is the set $\{x | x \in U \wedge x \notin A\} = \bar{A} = U - A$.

Definition (Relative Complement): For $A, B \subseteq U$, the **relative complement** of A in B is the set $\{x | x \in B \wedge x \notin A\} = B - A$.

Example 2: Suppose $U = \{1, 2, 3, \dots, 10\}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 4, 5, 6, 7\}$, and $C = \{7, 8, 9\}$. Determine the following sets:

$$\begin{array}{ll}
 B - A = \underline{\hspace{2cm}} & A - B = \underline{\hspace{2cm}} \\
 A - C = \underline{\hspace{2cm}} & C - A = \underline{\hspace{2cm}} \\
 U - A = \underline{\hspace{2cm}} & A - A = \underline{\hspace{2cm}}
 \end{array}$$

Theorem: For $A, B \subseteq U$, the following statements are equivalent:

$$A \subseteq B \quad A \cup B = B \quad A \cap B = A \quad \bar{B} \subseteq \bar{A}$$

4.2 Laws of Set Theory

We can adapt most of the laws already discussed in Section 3.4 for sets. For instance, both the union (\cup) and intersection (\cap) operations on sets satisfy commutative and associative laws of logic. Other common laws of logic for sets include the following identities, where the universe here is denoted U :

- | | |
|-----------------------------|--|
| 1. Distributive Laws | $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ |
| 2. Idempotent Laws | $A \cup A = A$
$A \cap A = A$ |
| 3. Identity Laws | $A \cup \emptyset = A$
$A \cap U = A$ |
| 4. Inverse Laws | $A \cup \bar{A} = U$
$A \cap \bar{A} = \emptyset$ |
| 5. Domination Laws | $A \cup U = U$
$A \cap \emptyset = \emptyset$ |
| 6. Absorption Laws | $A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$ |
| 7. DeMorgan's Laws for Sets | $\overline{(A \cup B)} = (\bar{A} \cap \bar{B})$
$\overline{(A \cap B)} = (\bar{A} \cup \bar{B})$ |

Definition (Principle of Set Duality): Let S be any identity made up of operations of \cup and \cap and any sets including \emptyset and U . Then the **dual** of the S denoted by S^d is defined by the following procedure:

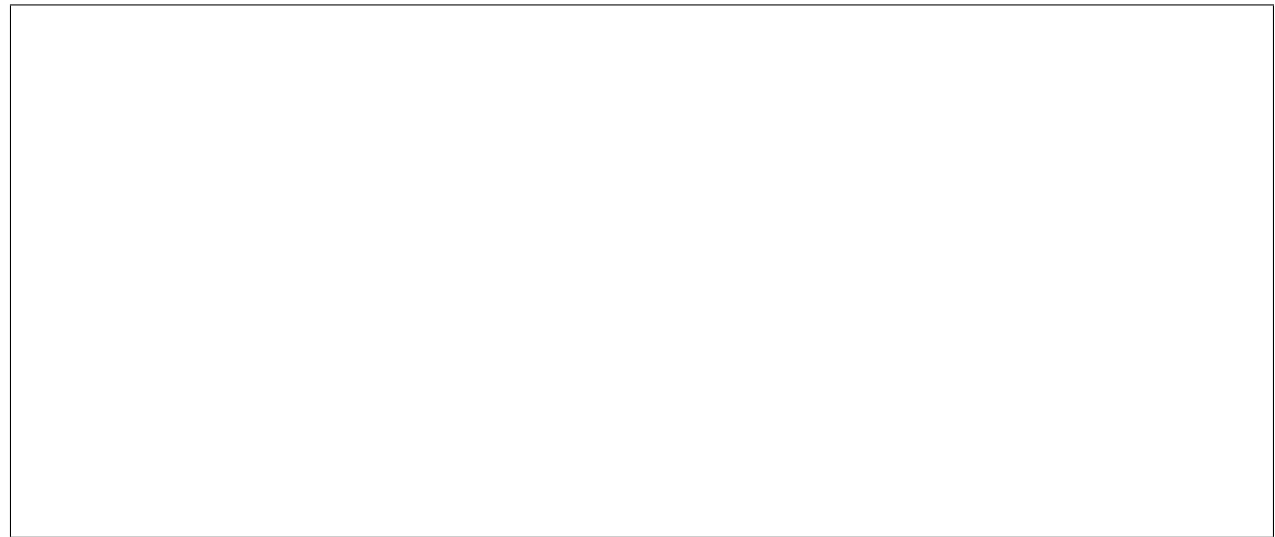
1. Replace every occurrence of \emptyset in S by the universe U and vice-versa.

2. Replace every occurrence of \cup by \cap in S and vice-versa.

The next theorem tells us that the dual, S_d , of an identity S is also an identity (i.e. a true statement) like the identities given above.

Theorem (Principle of Duality): The equality of two sets implies the equality of their respective dual sets.

Example 4: Simplify $\overline{[(A \cup B) \cap C] \cup \overline{B}}$.



In order to specify multiple unions or intersections of a *family* of sets, we utilize an index set I of nonnegative integers (e.g., $I = \mathbb{Z}^+$ is a typical index set). That is, for each $i \in I$, let $A_i \subseteq U$ for the universe U . A_i then forms what we call an *indexed family of sets* and we can then define the following:

Definition: The **union of an indexed family of sets**, A_i , is denoted and defined as

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i, \text{ for at least one } i \in I\} = \{x \mid \exists i \in I \text{ such that } x \in A_i\};$$

and the **intersection of an indexed family of sets**, A_i , is denoted and defined as

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for every } i \in I\} = \{x \mid \forall i \in I, x \in A_i\}.$$

Theorem (Generalized DeMorgan's Laws): Let I be an index set and in a universe U , let $A \subseteq U$. Then for $i \in I$ and $A_i \subseteq U$,

$$\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}, \text{ and } \overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i} .$$

5 MATHEMATICAL INDUCTION AND RECURSION

5.1 *The Principle of Mathematical Induction*

The Principle of Mathematical Induction is a very useful technique used to prove a proposition of the form “for all positive integers, n , $p(n)$ ” where $p(n)$ is an open proposition about n . (i.e. $\forall n \in \mathbb{Z}^+(p(n))$). (Also can be on the set $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$.)

Note: None of our proof methods so far can assist with proving such propositions and thus, this section introduces the Principle of Mathematical Induction which provides the method for a proof by induction.

Before formally stating the principle, we note that there are two main steps or parts to an induction proof and then illustrate the steps with an example of a proposition, $p(n)$ over the positive integers, \mathbb{Z}^+ .

- a. **The base case.** This step of an induction proof directly proves that the statement given as $p(n)$ is true for $n = n_0$ where n_0 is the smallest member of the set about which the statement is supposed to be true. (e.g., if we want to prove $p(n)$ over all the natural numbers, \mathbb{N} , then $n_0 = 0$; if instead we want to prove it is true over the infinite set $A = \{3, 4, 5, 6, \dots\}$, then $n_0 = 3$.)
- b. **The induction step.** This step relies on assuming that $p(k)$ is true for some k in the set under consideration and then using this to show that the statement $p(k + 1)$ is true. (i.e. prove that for some k in the set, $p(k) \rightarrow p(k + 1)$.) The assumption that $p(k)$ is true for some particular but arbitrary k in the set is known as the *induction hypothesis*.
- c. After these two steps are established, they are used along with the Principle of Mathematical Induction to conclude the statement $p(n)$ is true for all values n in the set being considered.

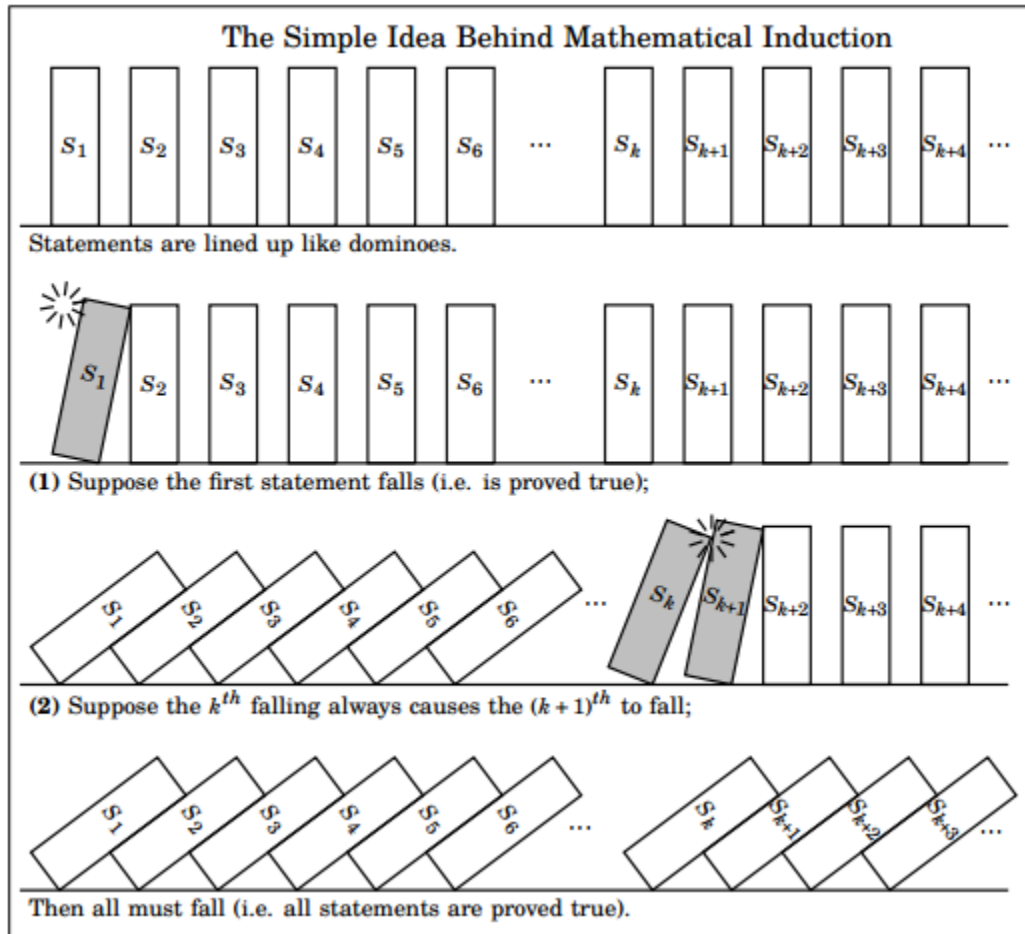


Figure 1: Illustration of the domino effect of the principle of mathematical induction. Image from: WillemsPlanet.com

Let's illustrate the two steps above for the following universally quantified proposition: $\forall n \in \mathbb{Z}^+, p(n)$, where $p(n)$ is the open proposition defined as:

$$p(n) := \sum_{i=1}^n i = \frac{n(n+1)}{2}.$$

Comments:

- $p(n)$ is a proposition that states the two expressions shown are equal to one another: the summation given from $i = 1$ to any $n \in \mathbb{Z}^+$ is the same as the formula given on the right in terms of n .
- The form of the universally quantified proposition, $\forall n \in \mathbb{Z}^+ P(n)$, fits the situation in which the Principle of Mathematical Induction is needed.

- The goal in proving this universally quantified proposition is to actually show that the left hand side of the equality statement in $p(n)$ (the summation) is equal to the right hand side of the equality (the formula) in $p(n)$ for all $n \in \mathbb{Z}^+$.

Now we illustrate how to carry out the two steps given above on this particular example:

Step 1 The Base Case: Check that $p(n)$ is a true statement for $n = n_0$, the smallest element in \mathbb{Z}^+ . Thus, let $n_0 = 1$. Then starting with the left hand side of the expression in $p(n)$ (i.e. the summation), we demonstrate that for $n = 1$, this is equal to the right hand side of the expression in $p(n)$ (i.e., the formula). Here, we do this by showing each expression is equal to the same value when $n = n_0 = 1$:

$$\sum_{i=1}^{n=n_0=1} i = 1 \quad \text{and} \quad \frac{n(n+1)}{2} = \frac{1(1+1)}{2} = \frac{1(2)}{2} = 1.$$

Therefore, the open proposition $p(n) := \sum_{i=1}^n i = \frac{n(n+1)}{2}$ is true for $n_0 = 1$ and the base case is proven.

Step 2 The induction step: for an arbitrarily but particular $n \in \mathbb{Z}^+$, prove that

$$p(n) \implies p(n+1).$$

Thus, assume that the premise $p(n)$ is true and proceed to show that $p(n+1)$ is true. Note that the *induction hypothesis* is that

$$p(n) := \sum_{i=1}^n i = \frac{n(n+1)}{2} \text{ is true for some } n \in \mathbb{Z}^+.$$

Recall that $p(n+1)$ is also an open proposition about equality of two expressions. So, first, examine what $p(n+1)$ is:

$$p(n+1) := \sum_{i=1}^{n+1} i = \frac{(n+1)((n+1)+1)}{2}.$$

Then, given this, we begin with the summation expression of the $p(n + 1)$ proposition and proceed to show this is equal to the formula expression in the proposition *using the induction hypothesis along the way*.

$$\begin{aligned}
 \sum_{i=1}^{n+1} i &= 1 + 2 + 3 + \cdots + n + (n + 1) \\
 &= \underbrace{(1 + 2 + 3 + \cdots + n)}_{\text{Look familiar?}} + (n + 1) \\
 &= \frac{n(n + 1)}{2} + (n + 1) \text{ using the induction hypothesis.} \\
 &= \frac{n(n + 1)}{2} + \frac{2(n + 1)}{2} \text{ (algebra)} \\
 &= \frac{n^2 + 3n + 2}{2} \text{ (algebra)} \\
 &= \frac{(n + 1)(n + 2)}{2} \text{ (algebra)} \\
 &= \frac{(n + 1)((n + 1) + 1)}{2}. \text{ (algebra)}
 \end{aligned}$$

Thus, we have shown that

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

which verifies the claim that $p(n) \implies p(n + 1)$, which is the induction step outlined above.

Having shown these two parts (the base case and the induction step), we can then use the Principle of Mathematical Induction to conclude that

$$\forall n \in \mathbb{Z}^+, \sum_{i=1}^n i = \frac{n(n + 1)}{2}.$$

It has already been stated above that we can *use* the Principle of Mathematical Induction (PMI), but to see why this is so, we now formally state and prove it, which requires us to also understand something about the

what it means for a set like \mathbb{Z}^+ to be *well-ordered*.

Well-Ordering Principle (WOP):

Every nonempty subset of \mathbb{Z}^+ contains a smallest element. (e.g., \mathbb{Z}^+ and $\{3, 4, 5, 6, \dots\}$ are examples of **well ordered** sets as is \mathbb{N} which essentially is the union of $\{0\}$ with \mathbb{Z}^+ , and the idea of well-ordering is preserved.)

Principle of Mathematical Induction (PMI):

Let $S(n)$ be an open proposition with one or more occurrences of the variable n for $n \in \mathbb{Z}^+$. Let n_0 denote the smallest element in \mathbb{Z}^+ , i.e. $n_0 = 1$.

(a) If $S(n_0 = 1)$ is true, and

(b) if, whenever $S(k)$ is true for some arbitrary $k \in \mathbb{Z}^+$, this implies $S(k + 1)$ is also true (i.e. $\forall k \geq n_0 [S(k) \implies S(k + 1)]$),

then we can conclude that $S(n)$ is true $\forall n \in \mathbb{Z}^+$.

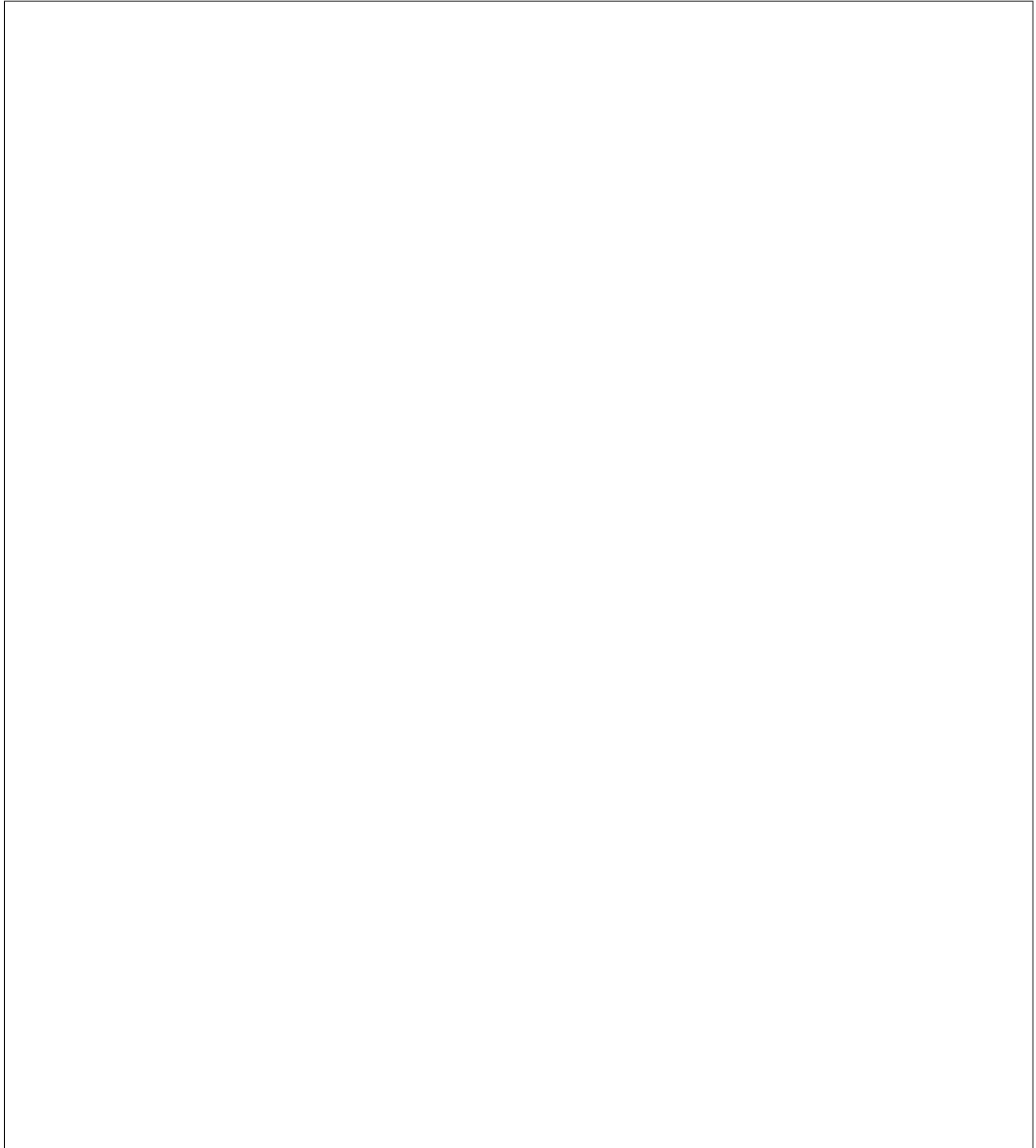
Proof. Assume $S(n)$ is an open proposition and the two conditions (a) and (b) above are satisfied. Note that $n_0 = 1$ is the smallest element of \mathbb{Z}^+ . Let $F = \{t \in \mathbb{Z}^+ \mid S(t) \text{ is false}\}$, the set of all values in \mathbb{Z}^+ for which $S(n)$ is false. We wish to show that $F = \emptyset$ and so, assume by way of contradiction that F is not empty. Since we are assuming F is not empty, by the WOP we know F has a smallest element, say m . Since $S(1)$ is true by condition (a), it then follows that $m \neq 1$. Additionally, since $n_0 = 1$ was the smallest element in \mathbb{Z}^+ , $m > 1$ and $m - 1 \in \mathbb{Z}^+$. Since $m - 1 < m$, we know that $m - 1 \notin F$ since we assumed m was the smallest element in F . Thus, since $m - 1 \notin F$, we have that $S(m - 1)$ is true. Therefore, by condition (b) $S(m - 1 + 1)$ is also true, i.e. $S(m)$ is true; however, this implies that $m \in F$ and so we have a contradiction. Our assumption that $F \neq \emptyset$ is false and so F must be empty meaning that $S(n)$ is true $\forall n \in \mathbb{Z}^+$. \square

A more symbolic representation of PMI would be

$$[S(n_0) \wedge [\forall k \geq n_0 [S(k) \implies S(k + 1)]]] \implies \forall n \geq n_0, S(n),$$

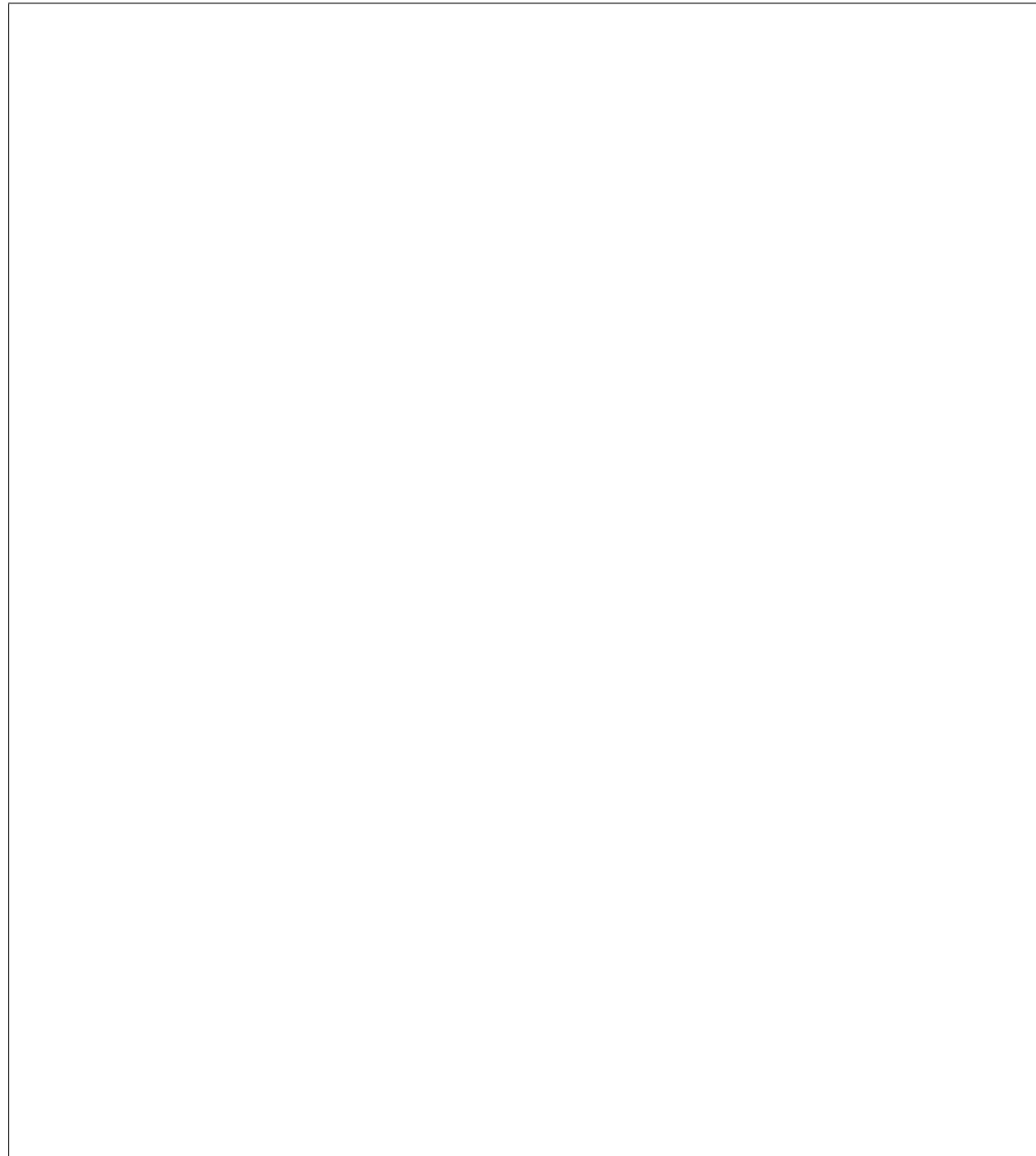
where $S(n_0)$ denotes the “base case.”

Example 1: Verify the formula $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$, holds $\forall n \in \mathbb{Z}^+$.



Example 2: Let's verify that the following is true:

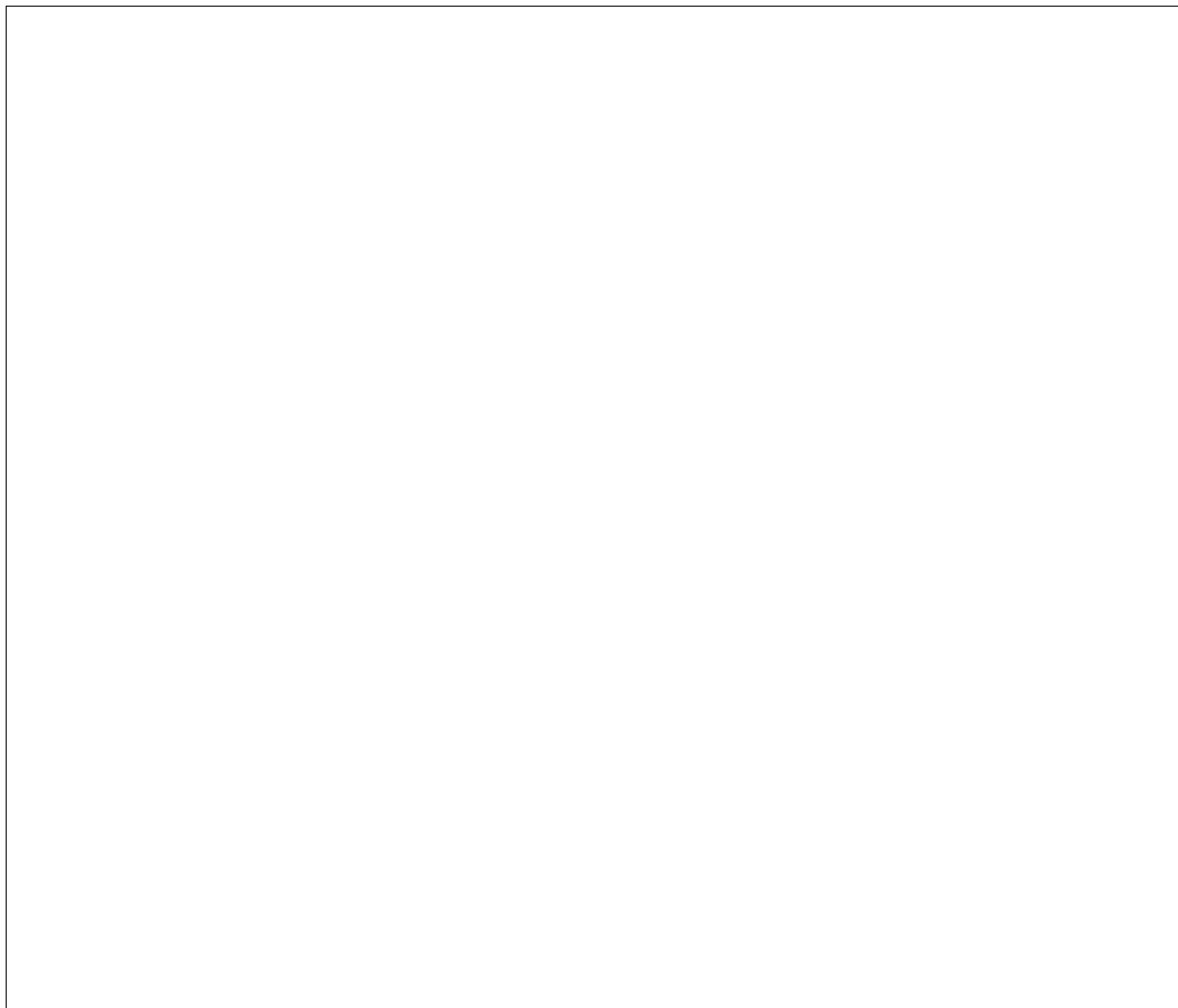
$$\forall n \in \mathbb{Z}^+, \sum_{i=1}^n i = 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$



Example 3: Suppose we want to construct a formula to sum consecutive odd positive integers:

$$\begin{aligned}1 &= 1 &= 1^2 \\1+3 &= 4 &= 2^2 \\1+3+5 &= 9 &= 3^2 \\1+3+5+7 &= 16 &= 4^2\end{aligned}$$

This pattern suggests that $S(n)$ defined as $\sum_{i=1}^n (2i - 1) = n^2$ would be a good candidate for the desired formula. Use the PMI to verify this formula.



Example 4: (Program Verification/Software Engineering) Consider the following *pseudocode* to compute $x(y^n)$ for real (float) variables x , y , and nonnegative integer n :

```
while n  $\neq$  0 do
  begin
    x:=x*y
    n:=n-1
  end
answer := x
```

Define $S(n)$ as follows: $\forall x, y \in \mathbb{R}$ if program reaches the top of the while loop with $n \in \mathbb{N}$ after the loop is by-passed (if $n = 0$) or the two loop instructions are executed $n (> 0)$ times, the value of the variable `answer` is $x(y^n)$.

Consider $S(0)$, i.e., the code doesn't enter the loop and `answer` will contain the value of x and that is equivalent to $x(y^0)$ so $S(0)$ is true.

Our induction hypothesis is that $S(k)$ is true for some $k \in \mathbb{Z}^+$: `answer` variable is $x(y^k)$ after the loop ends.

Now consider the proposition $S(k+1)$: `answer` = $x(y^{k+1})$. When the program reaches the top of the loop, $n = k + 1 > 0$ for the first time and the current value of x by the induction hypothesis is $x = x * (y^k)$. Thus, we have the new assignment of x as $x = x * y = x * (y^k) * y = x * (y^k * y) = x * y^{k+1}$ which gets assigned to the variable `answer`.

```
while n  $\neq$  0 do
  begin
    x:=x*y
    n:=n-1
    (memory trace)
  end
answer := x
```


Memory Trace: (at end of loop):

&x	&y	&n	
xy	y	$n - 1$	$S(1)$
xy^2	y	$n - 2$	$S(2)$
xy^3	y	$n - 3$	$S(3)$
\vdots	\vdots	\vdots	\vdots
xy^k	y	$n - k$	$S(k)$
xy^{k+1}	y	$n - (k + 1)$	$S(k + 1)$
\vdots	\vdots	\vdots	\vdots
xy^{n-1}	y	1	$S(n - 1)$
xy^n	y	0	$S(n)$

5.2 Recursive Definitions

A recursive definition for a sequence a_n :

Let $a_0 = 1$, $a_1 = 2$, $a_2 = 3$ and define $\forall n \in \mathbb{Z}^+$, $n \geq 3$,

$$a_n = a_{n-1} + a_{n-2} + a_{n-3}.$$

Now, consider the following equivalent compound propositions: $P_1 \wedge (P_2 \wedge P_3) \Leftrightarrow (P_1 \wedge P_2) \wedge P_3$. Each is equivalent to $P_1 \wedge P_2 \wedge P_3$. However, how would we use parenthesis to evaluate a compound proposition such as: about $P_1 \wedge P_2 \wedge P_3 \wedge P_4$?

Recursive Definition:

1. The conjunction of $P_1 P_2$ is defined by $P_1 \wedge P_2$.
2. Define $P_1 \wedge P_2 \wedge \dots \wedge P_n \wedge P_{n+1} \Leftrightarrow (P_1 \wedge P_2 \wedge \dots \wedge P_n) \wedge P_{n+1}$.

Does position really matter for \wedge ? It seems appropriate for the following chain of equivalences to be true:

$P_1 \wedge P_2 \wedge P_3 \wedge P_4 \Leftrightarrow (P_1 \wedge P_2 \wedge P_3) \wedge P_4 \Leftrightarrow P_1 \wedge (P_2 \wedge P_3 \wedge P_4) \Leftrightarrow (P_1 \wedge P_2) \wedge (P_3 \wedge P_4)$. This leads to the following law, the proof of which (not shown) utilizes idea of recursion and the Principle of Mathematical Induction.

Generalized Association Law for \wedge :

Let $n \in \mathcal{Z}^+$ where $n \geq 3$ and $r \in \mathcal{Z}^+$ with $1 \leq r \leq n$. For any statements

$$\begin{aligned} &P_1 P_2 \dots P_r P_{r+1} \dots P_n \\ &(P_1 \wedge P_2 \wedge \dots \wedge P_r) \wedge (P_{r+1} \wedge \dots \wedge P_n) \\ &\Leftrightarrow P_1 \wedge P_2 \wedge \dots \wedge P_r \wedge P_{r+1} \wedge \dots \wedge P_n \end{aligned}$$

Applying the above for set unions (and analogously for set intersections), we have: Given $A_1, A_2, \dots, A_n, A_{n+1}$ with $A_i \subseteq U$ for $1 \leq i \leq n+1$.

1. The union of A_1, A_2 is $A_1 \cup A_2$.
2. The union of $A_1, A_2, \dots, A_n, A_{n+1}$ for $n \geq 2$ is

$$A_1 \cup A_2 \cup \dots \cup A_n \cup A_{n+1} = (A_1 \cup A_2 \cup \dots \cup A_n) \cup A_{n+1}.$$

Example 1: Recall that $\sum_{r=0}^n \binom{n}{r} = \sum_{r=0}^n C(n, r) = 2^n$.

This is the number of subsets for a set of size n . A useful (and easy to verify) recursive definition for $C(n+1, r)$ is given by

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1} \text{ for } n \geq r \geq 0.$$

Example 2: (Recursively Defined Sets)

$X :=$

- (i) $1 \in X$, and
- (ii) $\forall a \in X, a+2 \in X$.

$E :=$

- (i) $2 \in E$, and
- (ii) $\forall n \in E, n+2 \in E$.

$G :=$

- (i) $0 \in G$, and
- (ii) $\forall m \in G, m+2 \in G$.

6 INTEGER PROPERTIES

6.1 Division Algorithm

Definition (Division): If $a, b \in \mathbb{Z}$ and $b \neq 0$, we say b divides a (we write $b|a$) if $\exists n \in \mathbb{Z}$ such that $a = bn$. We call b the *divisor* and say that a is a *multiple of b* .

Theorem: For $a, b, c \in \mathbb{Z}$

- a. $1|a$ and $a|0$
- b. $[(a|b) \wedge (b|a)] \implies a = \pm b$
- c. $[(a|b) \wedge (b|c)] \implies a|c$
- d. $a|b \implies a|bx, \forall x \in \mathbb{Z}$
- e. If $x = y + z$ for some $x, y, z \in \mathbb{Z}$ and a divides two of the three integers x, y, z , then a divides the third.
- f. $[(a|b) \wedge (a|c)] \implies a|(bx + cy) \forall x, y \in \mathbb{Z}$.
(Note: $bx + cy$ is called a *linear combination* of b and c)

Proof. If $a|b$ and $a|c$, then $b = am$ and $c = an$ for some $m, n \in \mathbb{Z}$. Then, $bx + cy = (am)x + (an)y = a(mx + ny)$. Since $mx + ny \in \mathbb{Z}$, we know $a|(bx + cy)$. \square

- g. For $1 \leq i \leq n$, let $c_i \in \mathbb{Z}$. If a divides c_i , then $a|(c_1x_1 + c_2x_2 + \cdots + c_nx_n)$, where $x_i \in \mathbb{Z}$ for all $1 \leq i \leq n$.

Example 1: Can we find $x, y, z \in \mathbb{Z}$ so that $6x + 9y + 15z = 107$? No, because $3|6, 3|9, 3|15$ so $3|6x + 9y + 15z$ but $3 \nmid 107$.

Example 2: Let $a, b \in \mathbb{Z}$ so that $2a + 3b$ is a multiple of 17. Let's use the above theorem to prove that 17 divides $9a + 5b$.

Proof. $17|(2a + 3b) \implies 17|(-4)(2a + 3b)$; Also, we know that $17|17$; so $17|(17a + 17b)$ as well (see Part f of Theorem above). Then $17|[(17a + 17b) + (-4)(2a + 3b)] \implies 17|(17a + 17b - 8a - 12b) \implies 17|(9a + 5b)$. \square

Definition (Primes): All integers in \mathbb{Z}^+ greater than 1 that have **exactly two divisors** are called primes. Examples: 2, 3, 5, 7, 11, 13, 17, ... All the other positive integers are called composites.

Lemma: If $n \in \mathbb{Z}$ and n is composite, then there is a prime number p such that $p|n$.

Proof. Let S be the set of all composite integers that have no prime divisors. If $S \neq \emptyset$, then by WOP, we know S has a least element m . If m is composite, then we can write $m = m_1m_2$ where $m_1, m_2 \in \mathbb{Z}^+$ with $1 < m_1 < m$ and $1 < m_2 < m$. Since $m_1 \notin S$ (because m is the least element of S) we know that m_1 must be prime or is divisible by a prime. In the latter case, there would exist a prime p such that $p|m_1$. But $m = m_1m_2$ so we also have $p|m$ as well, which is a contradiction since we assume $m \in S$. Therefore $S = \emptyset$. Thus if $n \in \mathbb{Z}$ is composite, then there exists p , a prime, such that $p|n$. \square

Theorem (Euclid's): There are infinitely many primes (4th century BC).

Proof. Assume there are a finite number of primes and list them as $p_1, p_2, p_3, \dots, p_k$. Let $B = (p_1 \times p_2 \times \dots \times p_k) + 1$. Since $B > p_i, \forall i \leq k$, B cannot be prime (hence composite). So by the Lemma (above), $\exists p_j$ with $1 \leq j \leq k$ and $p_j|B$. Since $p_j|B$, and $p_j|(p_1 \times p_2 \times \dots \times p_k)$ then p_j must divide 1 (previous Theorem Part e). That means p_j cannot be prime – a contradiction. Therefore, there must be an infinite number of primes. \square

Theorem (Division): If $a, b \in \mathbb{Z}$ with $b > 0$, \exists a unique $q, r \in \mathbb{Z}$ with $a = qb + r$, $0 < r < b$. We call q the *quotient* and r the *remainder*.

Pseudocode for Integer Division (for b dividing a):

```

int divide(a,b){
  if a = 0 then
    quotient := 0
    remainder := 0
  else
    r := abs(a)
    q := 0
    while r  $\geq$  b
      r := r - b
      q := q + 1
    end
    if a > 0 then
      quotient := q
      remainder := r
    else if r = 0 then
      quotient := -q
      remainder := 0
    else
      quotient := -q - 1
      remainder := b - r
    end
  end
end
}

```

Example 3: Let's trace the execution of the pseudocode above for $4 \mid (-12)$:

a	b	r	q
-12	4	12	0
		8	1
		4	2
		0	3

Thus, the quotient becomes -3 and the remainder is 0.

Example 4: Complete the trace (execution) table below for $4|(-11)$:

a	b	r	q
-11	4	11	0

Example 5: A grocery store runs a weekly contest. Each customer who purchases more than \$20 worth of groceries receives a game card with 12 numbers on it. If **any** of the numbers on the game card sum to exactly 500, then the customer wins a \$500 shopping spree at the store. Suppose Elena buys \$22.83 at the store and her card has the following numbers:

144, 336, 30, 66, 138, 162, 318, 54, 84, 288, 126, 468

.
Does Elena win?

6.2 Greatest Common Division (Euclidean Algorithm)

Definition (Common Divisor): For $a, b \in \mathbb{Z}$, a positive integer c is said to be a **common divisor** of a and b if $c|a$ and $c|b$.

Now if either $a \neq 0$ or $b \neq 0$ then $c \in \mathbb{Z}^+$ is called the **greatest common divisor** (gcd) of a, b if

1. $c|a$ and $c|b$, and
2. for any common divisor of a and b , say d , we have $d|c$.

Example 1: The common divisors of 42 and 70 are 1, 2, 7, 14. Thus, $\gcd(42, 70) = 14$.

Theorem (gcd): For $a, b \in \mathbb{Z}^+$, \exists a unique $c \in \mathbb{Z}^+$ such that $c = \gcd(a, b)$.

Important Properties:

1. $\gcd(a, b) = \gcd(b, a)$.
2. $\forall a \in \mathbb{Z}$, if $a \neq 0$ then $\gcd(a, 0) = |a|$.
3. For $a, b \in \mathbb{Z}^+$, $\gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$.
4. $\gcd(0, 0)$ is undefined.
5. $c = \gcd(a, b)$ is the smallest possible integer that can be written as a linear combination of a and b (from uniqueness of gcd proof)
6. a, b are called *relatively prime* when $\gcd(a, b) = 1$ (i.e., There is no integer greater than 1 that divides both a and b ; thus, $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1$).
7. If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.
8. If $a, b \in \mathbb{Z}^+$ and $c = ax + by$ for some $x, y \in \mathbb{Z}$, we cannot conclude that $c = \gcd(a, b)$.

Example 2: Since $\gcd(42,70) = 14 \exists x, y \in \mathbb{Z}$ such that $42x + 70y = 14$ or $3x + 5y = 1$. It is easy to check that $x = 2$ and $y = -1$ works but note that $\forall k \in \mathbb{Z}$ we can have:

$$\begin{aligned} 1 &= 3(2-5k) + 5(-1+3k), \\ 14 &= 42(2-5k) + 70(-1+3k). \end{aligned}$$

Theorem (Euclidean Algorithm): Let $a, b \in \mathbb{Z}^+$ and set $r_0 = a$ and $r_1 = b$. Apply the Division Algorithm n times as follows (assume $a > b$):

$$\begin{aligned} r_0 &= q_1 r_1 + r_2, \text{ for } 0 < r_2 < r_1 \text{ (start with } a/b) \\ r_1 &= q_2 r_2 + r_3, \text{ for } 0 < r_3 < r_2 \\ r_2 &= q_3 r_3 + r_4, \text{ for } 0 < r_4 < r_3 \\ &\vdots \\ r_i &= q_{i+1} r_{i+1} + r_{i+2}, \text{ for } 0 < r_{i+2} < r_{i+1} \\ &\vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, \text{ for } 0 < r_n < r_{n-1} \\ r_{n-1} &= q_n r_n \end{aligned}$$

The final nonzero remainder, r_n is $\gcd(a, b)$.

Example 3: Compute $\gcd(250,111)$ using the Euclidean Algorithm:

Example 4: Suppose a GTA helps a student debug a Java program in 6 minutes, but it takes 10 minutes to debug a C++ program. If the GTA works continuously for 104 minutes (and doesn't waste time), how many programs can he/she debug in each language?

Goal: We want integers $x, y \geq 0$ such that $6x + 10y = 104$. (This is called a *Diophantine equation* because it is a polynomial in which integer solutions are sought.)

6.3 *RSA Encryption*

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the encryption algorithm in 1978.

Modular arithmetic for integers is a wrap-around type of arithmetic operation as is used in our clock system. There are 24 hours in a day, and although the 24 hour convention of stating the time is sometimes used, often, instead of saying 13:00 for the hour after noon, we say 1:00. Thus, 1 is equivalent to 13 mod 12. Essentially, the 1 here is the remainder after dividing 13 by 12. Another example: 3 is equivalent to 1 mod 2 and 4 is equivalent to 0 mod 2.

Definition: Define the **set of integers modulo p (mod p)** as

$$\mathbb{Z}_p = \{0, 1, 2, \dots, p - 1\}.$$

Definition (Multiplicative Inverse): A **multiplicative inverse** (or MI) is a number when multiplied by x will equal 1 (written x^{-1}). So, $x \cdot x^{-1} = 1$.

Notable Fact: Two integers, x and p , with $x \in \mathbb{Z}_p$ have a gcd of 1 if and only if x has a MI in the modulo of p . i.e. $x \in \mathbb{Z}_p$ and $\gcd(x, p) = 1 \Leftrightarrow x^{-1} \in \mathbb{Z}_p$.

Example 1: $4 \in \mathbb{Z}_9$ and $\gcd(4, 9) = 1$ so 4 has a MI (4^{-1}) in mod 9. In fact, $4 \cdot 7 = 28 = 1 \pmod{9}$.

Not all integers will have MI's though. We know that $3 \in \mathbb{Z}_9$ but $\gcd(3, 9) \neq 1$. For any prime number p , every integer from 1 up to $p - 1$ has a gcd of 1 with p so therefore all those integers have a MI in modulo p .

Definition (Euler's Totient): The number of elements that have a MI in a set of modulo integers is called **Euler's Totient** and it is represented by the greek letter ϕ . In other words, ϕ is the number of elements that have their gcd with the modulus equal to 1. Let \mathbb{P} designate the set of all prime numbers. If $p \in \mathbb{P}$, then $\phi(p) = p - 1$.

Example 2: $\phi(7) = |\{1, 2, 3, 4, 5, 6\}| = 6$.

RSA is based on two algorithms:

1. Key generation (most complicated part; weak key generation makes RSA very vulnerable)
2. RSA Function Evaluation: a function F that takes input data x and a key k and produces either an encrypted result or plain text.

Steps to create secure RSA keys:

1. Select two large prime numbers p and q (at least 512 digits, 1024 digits preferred)
2. Generate modulus n by multiplying p and q (i.e., $n = p \times q$).
3. Calculate the totient $\phi(n) = (p - 1) \times (q - 1)$.
4. Generate a public key as a prime number calculated from the interval $[3, \phi(n)]$ that has a gcd of 1 with $\phi(n)$.
5. Generate a private key as in the inverse of the prime number selected in Step 4 (public key) with respect to mod $\phi(n)$.

Public Key: usually written as e , a prime number chosen in the range $[3, \phi(n)]$. In practice, $e = 65,537$ so that it has a high probability of a gcd of 1 with $\phi(n)$. This key is shared (not secret) so you don't want e to be a very large integer (desire efficient encryption). The public key is typically represented as the ordered pair (e, n) , where n is the modulus.

Private Key: Since the public key e has a gcd of 1 with $\phi(n)$, the MI of the public key with respect to $\phi(n)$ can be determined by the Euclidean Algorithm. The private key is then represented by the ordered pair (d, n) , where n is the modulus and $e \cdot d = 1 \pmod{\phi(n)}$.

RSA Function Evaluation: Let m represent the data/message (integers for now) and e be the public key. Then we encrypt the message via

$$F(m, e) = m^e \pmod{n}, \text{ where } n = p \times q$$

and $F(m, e)$ returns the ciphered message c . To decrypt the ciphered message c we use

$$F(c, d) = c^d \pmod{n}, \text{ so that } F(c, d) = m \text{ and } e \cdot d = 1 \pmod{\phi(n)}.$$

Example 3: Produce the ciphered word for *attack* using the following ASCII equivalent (base 10) integers for their respective letters:

$$a: 97 \quad c: 99 \quad k: 107 \quad t: 116$$

If we choose the primes $p = 17$ and $q = 37$ as the factors of $n = 629$, then $\phi(n) = 576$. A possible public key e such that $\gcd(e, \phi(n))$ is 1 is $e = 31$. We can then encode the word *attack* as follows:

$$\begin{aligned} a: 97 \quad & 97^{31} \bmod 629 = 384 \\ c: 99 \quad & 99^{31} \bmod 629 = 317 \\ k: 107 \quad & 107^{31} \bmod 629 = 330 \\ t: 116 \quad & 116^{31} \bmod 629 = 283 \end{aligned}$$

So, the word *attack* which would normally be represented by 97 116 116 97 99 107 is encoded as 384 283 283 384 317 330.

Knowing that the public key is $e = 31$, one can decode the first character (a) encoded as 384 only if the primes $p = 17$ and $q = 37$ are discovered. If that is the case, then one only needs to determine the private key d such that $e \cdot d = 1 \bmod \phi(n)$, where $\phi(n) = 576$. With the correct private key d , one can compute $F(384, d) = 97$ and decrypt the character a .

Let's use the Euclidean Algorithm (EA) to derive d using $e = 31$ and $\phi(n) = 576$.

The mathematics of RSA encryption is based on Euler's Theorem (1760) from the field of number theory. Euler proved that

$$x^{\phi(n)} \equiv 1 \pmod{n},$$

where $\phi(n)$ is Euler's Totient and x and n are relatively prime integers. If we have the private key d then, $c^d \equiv (m^e)^d \pmod{n}$. Therefore, $c^d \equiv m^{1+k\phi(n)} \equiv m \times 1 \equiv m \pmod{n}$.

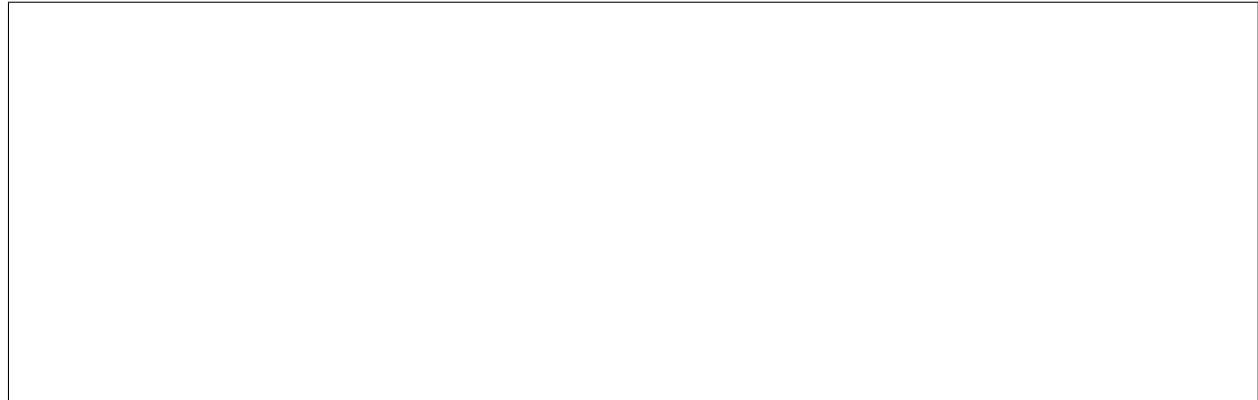
7 FUNCTIONS AND RELATIONS

We begin this section with definition of a few important sets that will be helpful in the creation of functions and relations.

7.1 Cartesian Products and Relations

Definition (Cartesian Product): Given sets A and B , the **Cartesian Product** or cross-product of A and B is defined by $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Example 1: Let $A = \{2, 3, 4\}$ and $B = \{4, 5\}$. Define $A \times B$, $B \times A$, and $B^2 = B \times B$.



Definition (Relation): Given sets A and B , any subset of $A \times B$ is called a (binary) **relation** from A to B . A subset of $A \times A$ is called a binary **relation on A** .

Example 2: If $|A \times B| = 6$, how many possible relations are there from A to B ? _____

For finite sets A and B with $|A| = m$ and $|B| = n$, there are 2^{mn} relations from A to B (this includes \emptyset and $A \times B$ itself). We have the same number of relations from B to A .

Example 3: Let $B = \{1, 2\}$ and $A = \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Is $\mathcal{R} = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\})\}$ a relation on A ? _____

Example 4: Let $A = \mathbb{Z}^+$ and define the relation \mathcal{R} on A as $\{(x, y) \mid x \leq y\}$.

Is $(7, 11) \in \mathcal{R}$? _____ Is $(8, 2) \in \mathcal{R}$? _____

Important Properties:

1. For any set A , $A \times \emptyset = \emptyset \times A = \emptyset$.
2. For $A, B \subseteq U$:
 - (a) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
 - (b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
 - (c) $(A \cap B) \times C = (A \times C) \cap (B \times C)$
 - (d) $(A \cup B) \times C = (A \times C) \cup (B \times C)$

7.2 Functions

Definition (Function): For nonempty sets A and B , a **function** or mapping f from A to B (denoted by $f : A \rightarrow B$) is a relation from A to B in which every element $a \in A$ appears *exactly once* as the first component of an ordered pair, (a, b) , for some $b \in B$.

Definition (Image): Given a function $f : A \rightarrow B$, for the ordered pair $(a, b) \in f$, we can write $f(a) = b$ and b is called the *image* of a under the function f .

Example 1: Let $A = \{1, 2, 3\}$ and $B = \{w, x, y, z\}$. Define $f = \{(1, w), (2, x), (3, x)\}$. Is f a function? _____ Now, define $\mathcal{R}_1 = \{(1, w), (2, x)\}$. Is \mathcal{R}_1 a function? _____ Consider $\mathcal{R}_2 = \{(1, w), (2, w), (2, x), (3, z)\}$. Is \mathcal{R}_2 a function? _____

Definition (Domain, Co-Domain, and Range): For a function $f : A \rightarrow B$, we call the set A the **domain** of f and the set B the **co-domain** of f . The **range** of f is the set $\text{Range}(f) \subseteq B$ containing all the images of A under f : $\text{Range}(f) = \{b \in B \mid \exists a \in A, f(a) = b\}$.

Common functions used in computer science applications:

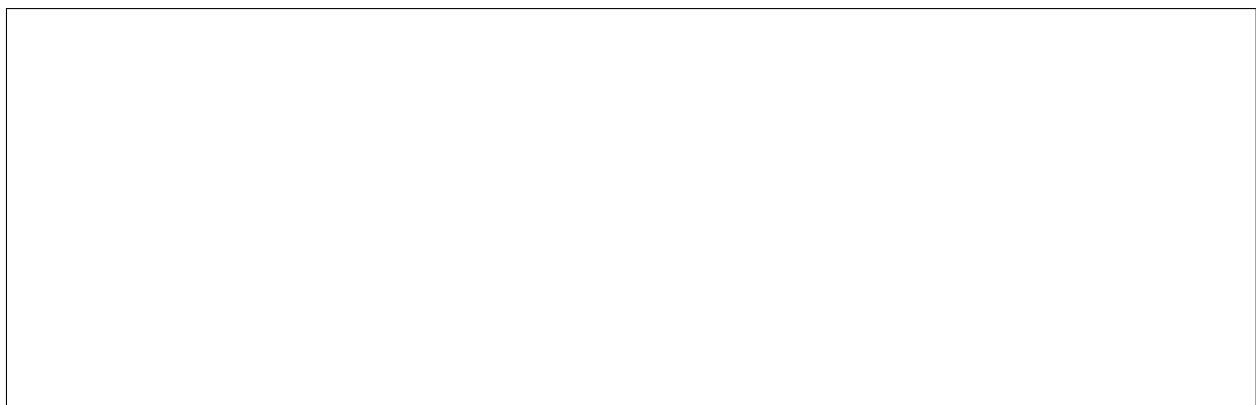
- a. **floor** defined by $f(x) = \lfloor x \rfloor$ is the greatest integer less than or equal to x . So $f(x) = x$ if $x \in \mathbb{Z}$ and for $x \in \mathbb{R} - \mathbb{Z}$ $f(x)$ is the integer to the immediate left on the real line. Examples: $\lfloor 3.8 \rfloor = 3$, $\lfloor -3.8 \rfloor = -4$, and $\lfloor -3 \rfloor = -3$.

- b. **ceiling** defined by $g(x) = \lceil x \rceil$ is the least integer greater than or equal to x . So $g(x) = x$ if $x \in \mathbb{Z}$ and for $x \in \mathbb{R} - \mathbb{Z}$ $g(x)$ is the integer to the immediate right on the real line. Examples: $\lceil 3.01 \rceil = 4$, $\lceil 3 \rceil = 3$, $\lceil 3.7 \rceil = 4$, $\lceil -3 \rceil = -3$, $\lceil -3.07 \rceil = -3$, and $\lceil -3.7 \rceil = -3$.
- c. **trunc** (or truncation) is the removal or deletion of the fraction. Examples: $\text{trunc}(3.78) = 3$ and $\text{trunc}(-7.22) = -7$. Note that $\text{trunc}(3.78) = \lfloor 3.78 \rfloor = 3$ and $\text{trunc}(-3.78) = \lceil -3.78 \rceil = -3$.
- d. 2D-array storage - it is common to store 2d logical arrays as 1D arrays in memory using row-major order access. Verify that the function $f(a_{ij}) = (i - 1) \times n + j$ will return the position (index) of the a_{ij} element in a 1D (or linear) array.

Example 2: Evaluate the following:

$$\begin{array}{ll} \lfloor 7.1 + 8.2 \rfloor & \underline{\hspace{2cm}} \\ \lfloor 7.7 + 8.4 \rfloor & \underline{\hspace{2cm}} \\ \lfloor 7.7 \rfloor + \lfloor 8.4 \rfloor & \underline{\hspace{2cm}} \\ \lceil 3.3 + 4.2 \rceil & \underline{\hspace{2cm}} \\ \lceil 3.3 \rceil + \lceil 4.2 \rceil & \underline{\hspace{2cm}} \end{array}$$

Definition (One-to-One or Injective Function): A function $f : A \rightarrow B$ is called **one-to-one (1-to-1)** or **injective** if every element of B appears at **most once** as the image of an element of A . i.e. The function f is 1-1 if $f(a_1) = f(a_2) \rightarrow a_1 = a_2$. Let's draw a diagram of a 1-to-1 function:



Example 3: Consider $f : \mathbb{R} \rightarrow \mathbb{R}$ and $g : \mathbb{R} \rightarrow \mathbb{R}$, where $f(x) = 3x + 7$, $\forall x \in \mathbb{R}$ and $g(x) = x^4 - x$, $\forall x \in \mathbb{R}$. Determine whether f and g are 1-to-1 functions?

Example 4: Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4, 5\}$. Suppose $f = \{(1, 1), (2, 3), (3, 4)\}$ and $g = \{(1, 1), (2, 3), (3, 3)\}$. Are both f and g 1-to-1 functions? _____

Example 5: Suppose set $A = \{a_1, a_2, \dots, a_m\}$ and set $B = \{b_1, b_2, \dots, b_n\}$ with $m \leq n$. Derive a formula for the number of 1-to-1 functions there are from set A to set B .

Theorem: Let $f : A \rightarrow B$ and $A_1, A_2 \subseteq A$.

- a. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
- b. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
- c. $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ if f is 1-to-1

Definition (Restriction, Extension): If $f : A \rightarrow B$ and $A_1 \subseteq A$ we define $f|_{A_1} : A_1 \rightarrow B$ and call $f|_{A_1}$ the **restriction** of the function f to the subset A_1 . So $\forall a \in A_1, f|_{A_1}(a) = f(a)$. Similarly, if $h : A_1 \rightarrow B$ and we define $g : A \rightarrow B$ with $g(a) = h(a), \forall a \in A_1$, then g is called the **extension** of the function h to the set A .

Example 6: Suppose set $A = \{1, 2, 3, 4, 5\}$ and we define $f : A \rightarrow \mathbb{Z}$ by

$$f = \{(1, 10), (2, 13), (3, 16), (4, 19), (5, 22)\}.$$

Define $g : \mathbb{Q} \rightarrow \mathbb{R}$ by $g(q) = 3q + 7, \forall q \in \mathbb{Q}$ and define $h : \mathbb{R} \rightarrow \mathbb{R}$ by $h(r) = 3r + 7, \forall r \in \mathbb{R}$. Fill in the blanks below to complete each statement.

- g is an extension of _____ from A to _____.
- f is the restriction of _____ from \mathbb{Q} to _____.
- h is an extension of _____ from A to _____.
- h is an extension of _____ from \mathbb{Q} to _____.
- f is the restriction of _____ from \mathbb{R} to A .
- g is the restriction of _____ from \mathbb{R} to \mathbb{Q} .

Example 7: Let $A = \{w, x, y, z\}$, $B = \{1, 2, 3, 4, 5\}$, and $A_1 = \{w, y, z\}$. Suppose $f = \{(w, 1), (x, 3), (y, 5), (z, 4)\}$ and $g = \{(w, 1), (y, 5), (z, 4)\}$. Clearly $g = f|_{A_1}$ or we could say that f is an extension of g from A_1 to A . How many ways can we expand g from A_1 to A ?

7.3 Onto Functions

Definition (Onto or Surjective Function): A function $f : A \rightarrow B$ is called **onto or surjective** if $f(A) = B$, i.e., $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

Note: If a function, $f : A \rightarrow B$, is onto, then $B = \text{Range}(f)$.

Example 1: $f : \mathbb{R} \rightarrow \mathbb{R}$ with $f(x) = x^3$ is onto but $g : \mathbb{R} \rightarrow \mathbb{R}$ with $f(x) = x^2$ is **not** onto. Which of the functions below are onto functions?

$$f : \mathbb{Z} \rightarrow \mathbb{Z} \text{ with } f(x) = 3x + 1, \forall x \in \mathbb{Z}.$$

$$g : \mathbb{Q} \rightarrow \mathbb{Q} \text{ with } g(x) = 3x + 1, \forall x \in \mathbb{Q}.$$

$$h : \mathbb{R} \rightarrow \mathbb{R} \text{ with } h(x) = 3x + 1, \forall x \in \mathbb{R}.$$

Example 2: Let $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z\}$. Which of the functions below are onto functions?

$$f_1 = \{(1, z), (2, y), (3, x), (4, y)\}$$

$$f_2 = \{(1, x), (2, x), (3, y), (4, z)\}$$

$$g = \{(1, x), (2, x), (3, y), (4, y)\}$$

An important observation for onto functions is that if A and B are **finite** sets and $f : A \rightarrow B$, then for f to be onto we must have $|A| \geq |B|$.

Example 3: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Are all functions $f : A \rightarrow B$ onto? How many onto functions are there from A to B ?

In general, if $|A| = m \geq 2$ and $|B| = 2$, then there are _____ onto functions from A to B .

Example 4: Let $A = \{w, x, y, z\}$ and $B = \{1, 2, 3\}$. There are 3^4 functions from A to B . For subsets of size 2, there are 2^4 functions from A to $\{1, 2\}$, 2^4 functions from A to $\{2, 3\}$ and 2^4 functions from A to $\{1, 3\}$. So, there are

$$3 \times 2^4 \text{ or } \binom{3}{2} \times 2^4$$

functions from A to B that are **not onto**. Let's derive the total number of onto functions there can be from A to B .

In general, for finite sets A and B with $|A| = m$ and $|B| = n$, there are

$$\sum_{k=0}^n (-1)^k \binom{n}{n-k} (n-k)^m$$

onto functions from A to B .

7.4 Function Composition and Inverse Functions

Definition (Bijective Function): A function $f : A \rightarrow B$ is called **bijective** or a **1-to-1 correspondence** if it is both 1-to-1 and onto.

Definition (Identity Function): The special function $1_A : A \rightarrow A$ defined by $1_A(a) = a \forall a \in A$ is called the **identity function on the set A** .

Definition (Function Equality): For functions $f, g : A \rightarrow B$, we say that f **equals** g and write $f = g$, if $f(a) = g(a)$, $\forall a \in A$.

Example 1: Suppose $f : \mathbb{Z} \rightarrow \mathbb{Z}$ and $g : \mathbb{Z} \rightarrow \mathbb{Q}$ such that $f(x) = x = g(x)$, $\forall x \in \mathbb{Z}$. Is $f = g$?

Example 2: Consider $f, g : \mathbb{R} \rightarrow \mathbb{Z}$ with $g(x) = \lceil x \rceil$, $\forall x \in \mathbb{R}$ and

$$f(x) = \begin{cases} x, & \text{if } x \in \mathbb{Z}, \\ \lceil x \rceil + 1, & \text{if } x \in \mathbb{R} - \mathbb{Z}. \end{cases}$$

Determine whether or not $f(x) = g(x)$, $\forall x \in \mathbb{R}$?

Definition (Composition of Functions): If $f : A \rightarrow B$ and $g : B \rightarrow C$, then the **composition of g with f** , $g \circ f$, is a function $g \circ f : A \rightarrow C$ and is defined by

$$(g \circ f)(a) = g(f(a)), \forall a \in A .$$

Example 3: Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$ and $C = \{w, x, y, z\}$. Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$, with $f = \{(1, a), (2, a), (3, b), (4, c)\}$ and $g = \{(a, x), (b, y), (c, z)\}$. Derive $g \circ f$ and evaluate $(g \circ f)(1)$, $(g \circ f)(2)$, $(g \circ f)(3)$, and $(g \circ f)(4)$.

Example 4: Suppose $f, g : \mathbb{R} \rightarrow \mathbb{R}$ with $f(x) = x^2$ and $g(x) = x + 5$. Determine $(g \circ f)(x)$ and $(f \circ g)(x)$. What can we say about the composition of functions and commutativity?

Theorem: Given $f : A \rightarrow B$ and $g : B \rightarrow C$.

- a. If f and g are **onto**, then $(g \circ f)$ is **onto**.
- b. If f and g are **1-to-1**, then $(g \circ f)$ is **1-to-1**.

Theorem: Given $f : A \rightarrow B$, and $g : B \rightarrow C$, and $h : C \rightarrow D$.

$$(h \circ g) \circ f = h \circ (g \circ f).$$

So, the composition of functions is **associative**.

Definition (Powers of Function): If $f : A \rightarrow A$, we define $f^1 = f$ and $f^{n+1} = f \circ f^n$ for $n \in \mathbb{Z}^+$. That is, powers are recursive applications of the same function.

Example 5: Suppose $A = \{1, 2, 3, 4\}$ and $f : A \rightarrow A$ with

$$f = \{(1, 2), (2, 2), (3, 1), (4, 3)\}.$$

Determine f^2 and f^3 .

Definition (Converse of a Relation): For sets A and B with a relation \mathcal{R} from A to B , the **converse** of \mathcal{R} (denoted by \mathcal{R}^c) is a relation from B to A defined as

$$\mathcal{R}^c = \{(b, a) \mid (a, b) \in \mathcal{R}\} .$$

Example 6: Suppose $A = \{1, 2, 3\}$ and $B = \{w, x, y\}$ with $f : A \rightarrow B$ defined by $f = \{(1, w), (2, x), (3, y)\}$. Derive f^c and compute $f^c \circ f$ and $f \circ f^c$.

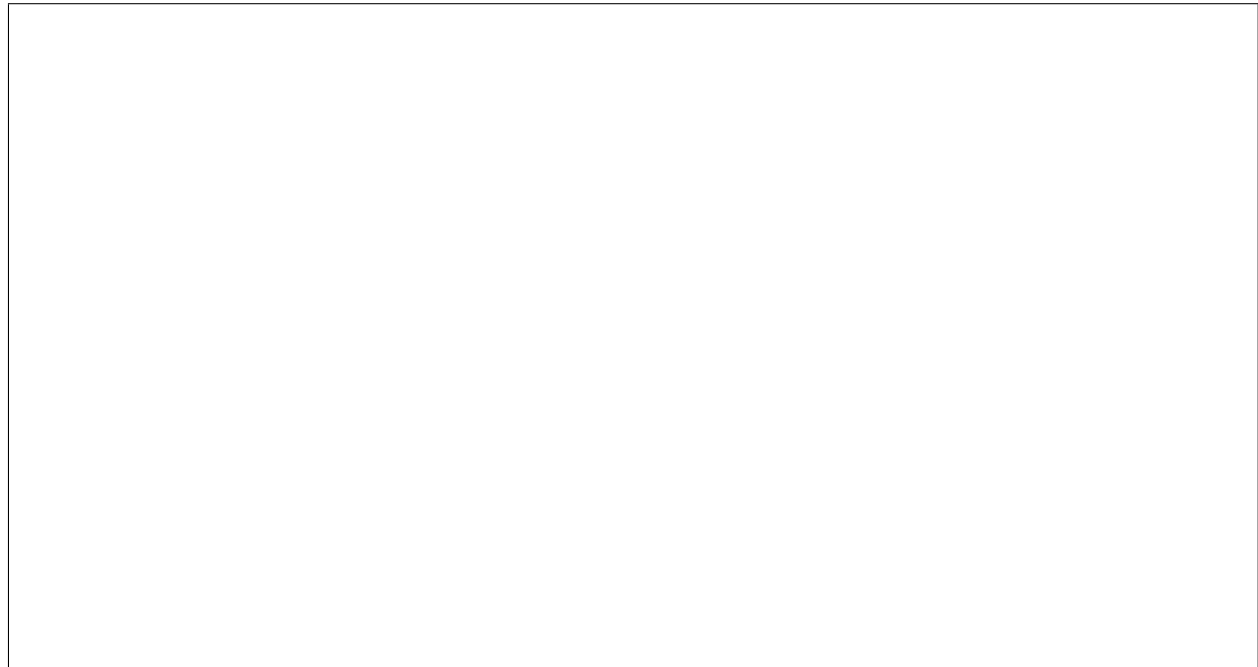
Definition (Invertible Function): If $f : A \rightarrow B$, then f is **invertible** if $\exists g : B \rightarrow A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. We call g the **inverse** of f denoted $g = f^{-1}$.

Example 7: Consider $f, g : \mathbb{R} \rightarrow \mathbb{R}$ with $f(x) = 2x + 5$ and $g(x) = (x - 5)/2$. Show that both f and g are invertible functions.

Theorem: A function $f : A \rightarrow B$ is **invertible** if and only if f is 1-to-1 and onto.

Example 8: Determine which of the following are invertible:

- a. $f_1 : \mathbb{R} \rightarrow \mathbb{R}$ with $f_1(x) = x^2$.
- b. $f_2 : [0, \infty+) \rightarrow [0, \infty+]$ with $f_2(x) = x^2$.



Theorem: If $f : A \rightarrow B$ and $g : B \rightarrow C$ are both **invertible**, then $g \circ f : A \rightarrow C$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

When $f : A \rightarrow B$ is not invertible, we can still define the set given by f^{-1} but it will not represent an inverse function.

Definition (Preimage): If $f : A \rightarrow B$, and $B_1 \subseteq B$, then

$$f^{-1}(B_1) = \{x \in A \mid f(x) \in B_1\} .$$

We call $f^{-1}(B_1)$ the **preimage** of B_1 under the function f .

Example 9: Let $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{6, 7, 8, 9, 10\}$. Suppose $f : A \rightarrow B$ with $f = \{(1, 7), (2, 7), (3, 8), (4, 6), (5, 9), (6, 9)\}$. Is f 1-to-1? _____
Is f onto? _____.

Determine $f^{-1}(B_1)$ and $|f^{-1}(B_1)|$ for each of the cases of B_i below:

- a. $B_1 = \{6, 8\}$
- b. $B_2 = \{7, 8\}$
- c. $B_3 = \{8, 9\}$
- d. $B_4 = \{8, 9, 10\}$
- e. $B_5 = \{8, 10\}$

Theorem: If $f : A \rightarrow B$ and $B_1, B_2 \subseteq B$, then

- a. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
- b. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
- c. $f^{-1}(\overline{B_1}) = \overline{f^{-1}(B_1)}$

Theorem: If $f : A \rightarrow B$ for finite sets A and B with $|A| = |B|$, then the following are all equivalent:

- a. f is 1-to-1,
- b. f is onto, and
- c. f is invertible.

7.5 Computational Complexity

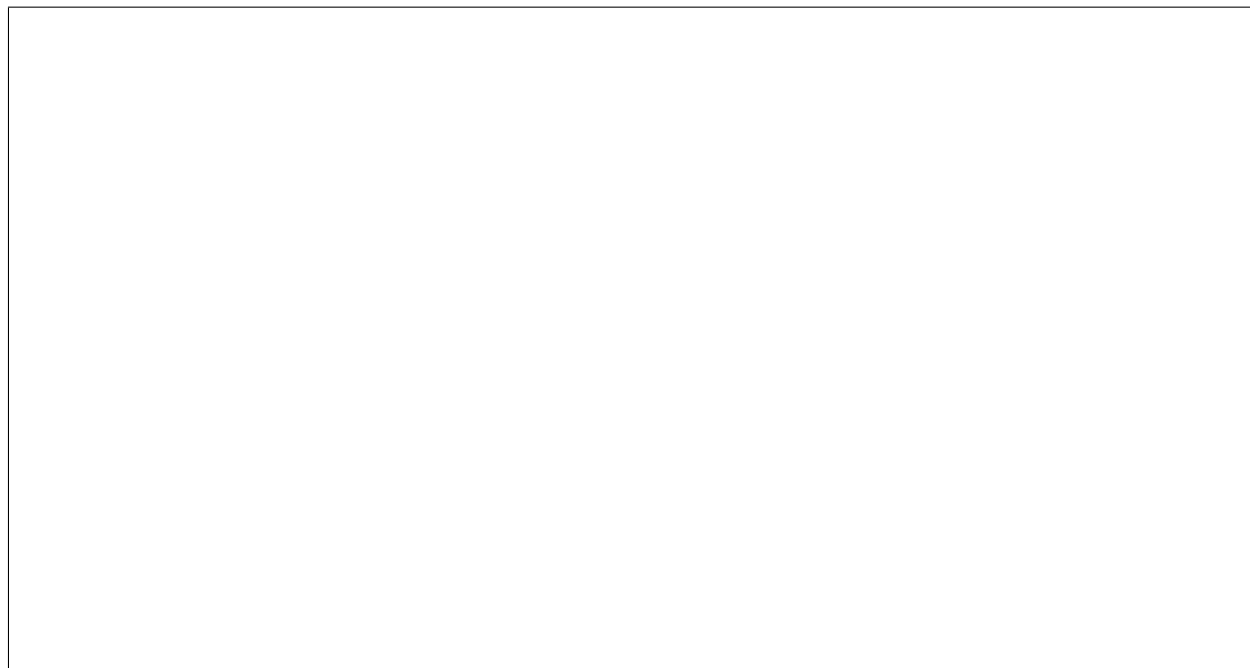
How can we determine the runtime of an algorithm ahead of time and how do we compare the runtime of different algorithms? Let $f(n)$ be the time complexity function for a given algorithm.

Definition (Dominated Function): Let $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$. We say that the function g **dominates** the function f if there exists constants $m \in \mathbb{R}^+$ and $k \in \mathbb{Z}^+$ such that

$$|f(n)| \leq m|g(n)|, \forall n \in \mathbb{Z}^+ \text{ and } n \geq k.$$

When f is **dominated** by g we say that f is of **order** (at most) g and write $f \in \mathcal{O}(g)$. We can think of $\mathcal{O}(g)$ as the set of all functions having domain \mathbb{Z}^+ and co-domain \mathbb{R} that are dominated by g .

Example 1: Consider $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$ with $f(n) = 5n$ and $g(n) = n^2$, $\forall n \in \mathbb{Z}^+$. Show that $f \in \mathcal{O}(g)$.



Now, prove that $g \notin \mathcal{O}(f)$.

Example 2: Consider $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$ with $f(n) = 5n^2 + 3n + 1$ and $g(n) = n^2, \forall n \in \mathbb{Z}^+$. Show that $f \in \mathcal{O}(g)$ and $g \in \mathcal{O}(f)$.

In general, if

$$f(n) = a_t n^t + a_{t-1} n^{t-1} + \cdots + a_2 n^2 + a_1 n + a_0,$$

where the a_i 's $\in \mathbb{R}$, $a_t \neq 0$, and $t \in \mathbb{N}$, then $\mathcal{O}(f) = \mathcal{O}(n^t)$.

Example 3: Consider $f, g : \mathbb{Z}^+ \rightarrow \mathbb{R}$ with $f(n) = 1 + 2 + \cdots + n$ and $g(n) = 1^2 + 2^2 + \cdots + n^2$. How do we know that $f \in \mathcal{O}(n^2)$ and $g \in \mathcal{O}(n^3)$?

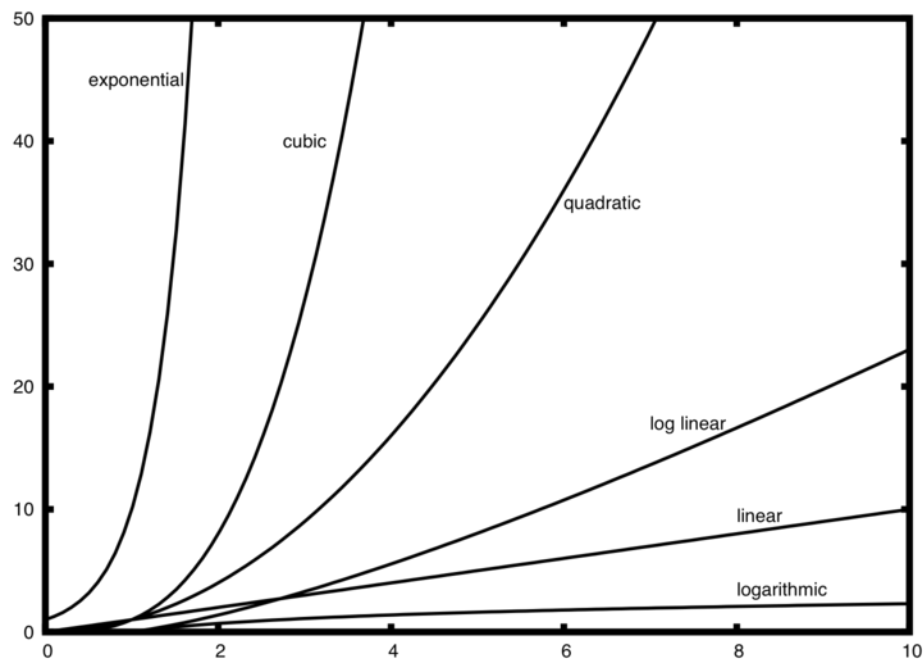
Example 4: If $h : \mathbb{Z}^+ \rightarrow \mathbb{R}$ with $h(n) = \sum_{i=1}^n i^t$, determine $\mathcal{O}(h(n))$.

Important time complexities:

BigOh	Name
$\mathcal{O}(1)$	constant
$\mathcal{O}(\log_2 n)$	logarithmic
$\mathcal{O}(n)$	linear
$\mathcal{O}(n \log_2 n)$	$n \log_2 n$
$\mathcal{O}(n^2)$	quadratic
$\mathcal{O}(n^3)$	cubic
$\mathcal{O}(n^t)$	polynomial (for $t = 0, 1, 2, \dots$)
$\mathcal{O}(c^n)$	exponential ($c > 1$)
$\mathcal{O}(n!)$	factorial

For purposes of comparison, let's complete the following table of entries:

n	$\log_2 n$	$n \log_2 n$	n^2	2^n	$n!$
2	1	2	4	4	2
16	4	64	256	_____	_____
64	6	384	4096	_____	_____



Example 5: Determine the runtime complexity of the following C++ code fragments:

```
sum=0; // fragment 1
for (i=0; i < n; i++) {
    for (j=0; j < n; j++) {
        sum=sum+1; } }
```

```
sum=0; // fragment 2
i=n;
while (i > 0) {
    sum=sum+1;
    i=floor(i/2); }
```

```
sum=0; // fragment 3
for (i=0; i < n; i++) {
    j=n;
    while (j > 0) {
        sum=sum+1;
        j=floor(j/2); } }
```

Example 6: Determine the runtime complexity of the following C++ function power that computes x^n , where both x and n are integers.

```
long power (long x, long n)
    if (n==0) return 1;
    else
        return x * power(x, n-1);
```

This is a recursive function obviously and we desire the runtime $T(n)$ for any input (integer) exponent n . We can see that initially (for $n = 0$) we have $T(0) = c_1$, for some constant c_1 . From the code, we have the recurrence relation

$$T(n) = c_2 + T(n - 1),$$

where c_2 is another constant. Notice that we could write

$$T(n) = T(n - 1) + c_2 = T(n - 2) + c_2 + c_2 = T(n - 2) + 2c_2.$$

Continue this process of writing the left-hand-side of the recurrence in terms of previous recursive calls to power until you can write $T(n)$ in terms of any previous call to power, say the k -th.

We then conclude that the big-oh runtime for power is _____.

Example 7: Let's determine the runtime complexity of the following (improved) C++ function power that computes x^n , where both x and n are integers and n is a power of 2.

```
long power (long x, long n)
    if (n==0) return 1;
    if (n==1) return x;
    if ( (n % 2) == 0)
        return power(x*x, n/2);
    else
        return x * power(x*x, n/2);
```

As with the previous example, we need to define a recurrence relation for the runtime of consecutive calls to the recursive function power. Initially, we have $T(0) = c_1$ and $T(1) = c_2$, for constants c_1 and c_2 . From the code, we have the recurrence relation

$$T(n) = T(n/2) + c_3,$$

where c_3 is yet another constant. Notice that we could write

$$T(n) = T(n/2) + c_3 = T(n/4) + c_3 + c_3 = T(n/4) + 2c_3.$$

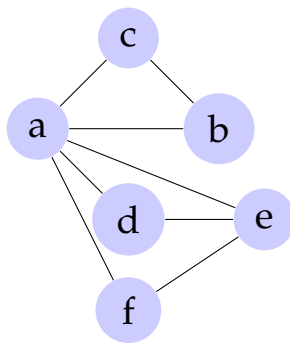
Continue this process of writing the left-hand-side of the recurrence in terms of previous recursive calls to power until you can write $T(n)$ in terms of any previous call to power, say the k -th.

We then conclude that the big-oh runtime for the modified power function is _____.

8 GRAPH THEORY

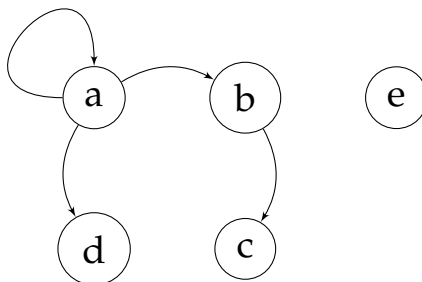
8.1 Introduction

Definition: Let V be a finite nonempty set and $E \subset V \times V$. The pair (V, E) is called a **directed graph** on V or a digraph on V . V (the vertex set) is the set of vertices or nodes. E (the edge set) is the set of directed edges or arcs. We define the graph G by $G = (V, E)$. If the edges in E need no direction, then G is called an **undirected graph**.



In the graph above we have, $V = \{a, b, c, d, e, f\}$ and $E = \{\{a, c\}, \{a, b\}, \{a, d\}, \{d, e\}, \{a, f\}, \{f, e\}, \{a, e\}, \{b, c\}\}$.

An example of a directed graph is given below:

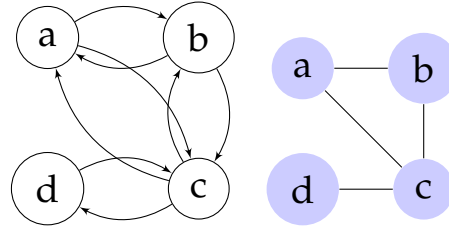


Here, we have $V = \{a, b, c, d, e\}$ and $E = \{(a, a), (a, b), (a, d), (b, c)\}$. Given edge (b, c) , vertex b is the origin or **source** vertex and vertex c is called the terminus or **terminating** vertex. The edge (a, a) is a **loop**, and vertex e (which has no incident edges) is called an **isolated** vertex.

In some cases, an undirected graph is used as a more compact way to

describe a directed graph.

Example 1: The directed graph on the left is recast as an undirected graph on the right:



Notice that $\{a, b\}$ (an edge in the undirected graph) is equivalent to $\{(a, b), (b, a)\}$ (the corresponding edge in the directed graph). Regarding loops, we can write $\{a, a\} = (a, a)$. Generally, we assume a graph is undirected (if not specified) and if the graph has no loops, we refer to it as being **loop-free**.

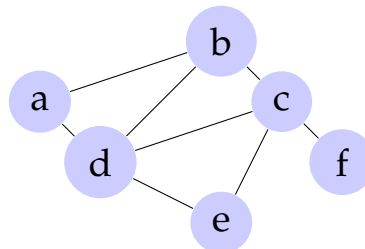
Definition: Let x, y be two vertices in an undirected graph, $G = (V, E)$, with x and y not necessarily distinct. An x - y **walk** in G is a **loop-free** alternating sequence:

$$x = x_0, e_1, x_1, e_2, x_2, e_3, \dots, e_{n-1}, x_{n-1}, e_n, x_n = y,$$

with $e_i = \{x_{i-1}, x_i\}$, $1 \leq i \leq n$. The length of the walk is the number of edges traversed (n edges). If $n = 0$, we considered it a **trivial** walk.

Definition: Any x - y walk, where $x = y$ and $n > 1$ is a **closed walk**; otherwise it is an **open walk**.

Example 2: Consider the 6-vertex undirected graph below:



Possible walks in this graph include:

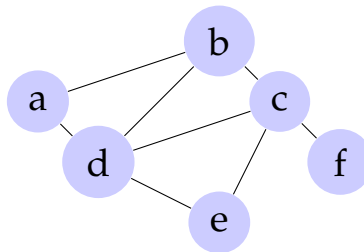
1. The a - b walk of length 6: $\{a, b\}, \{b, d\}, \{d, c\}, \{c, e\}, \{e, d\}, \{d, b\}$
2. The b - f walk of length 5: $b \rightarrow c \rightarrow d \rightarrow e \rightarrow c \rightarrow f$

3. The f - a walk of length 4: $\{f, c\}, \{c, e\}, \{e, d\}, \{d, a\}$
4. The **closed** walk b - b : $\{b, c\}, \{c, d\}, \{d, b\}$

Definition: Let x - y be a walk in the undirected graph $G = (V, E)$.

- a. If no edge in x - y walk is repeated, then x - y walk is called an x - y **trail**.
- b. A closed x - x trail is called a **circuit**. We will assume all circuits of interest have at least one edge.
- c. If no vertex of an x - y walk occurs more than once, then walk is called an x - y **path**. When $x = y$, the closed path is called a **cycle**.

Example 3: Let's return to the same undirected graph we had in Example 2:

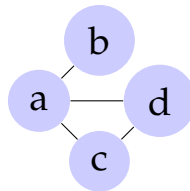


- Is the b - f walk from above a trail? _____
- Is that same b - f walk a path? _____
- Is $\{a, b\}, \{b, d\}, \{d, c\}, \{c, e\}, \{e, d\}, \{d, a\}$ a circuit? _____ Is it a cycle? _____
- Are all the cycles b - b , c - c , d - d with more than 2 vertices also circuits? _____

Summary:

Repeated Vertices	Repeated Edges	Open	Closed	Name
y	y	y	n	Open Walk
y	y	n	y	Closed Walk
y	n	y	n	Trail
y	n	n	y	Circuit
n	n	y	n	Path
n	n	n	y	Cycle

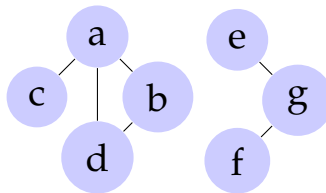
Theorem Let $G = (V, E)$ be an undirected graph with $a, b \in V$. If \exists a trail in G from a to b , then there is a path in G from a to b . Consider the 4-vertex undirected graph below:



Here, we have the trail $a \rightarrow c \rightarrow d \rightarrow a \rightarrow b$.

Definition (Connected Graph): Let $G = (V, E)$ be an undirected graph. We say that G is **connected** if there is a path between any two distinct vertices of G . If G is not connected, then G is **disconnected**.

Consider the 7-vertex (undirected) disconnected graph below that has two connected components:

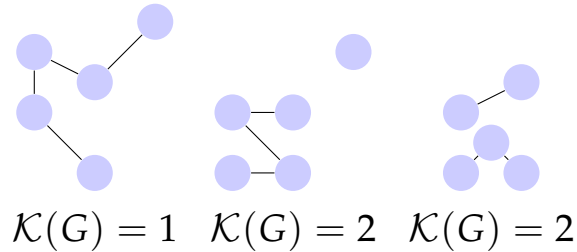


In the graph, we see the complete vertex set $V = \{a, b, c, d, e, f, g\}$ and two vertex subsets $V_1 = \{a, b, c, d\}$ and $V_2 = \{e, f, g\}$. The corresponding edge sets for V_1 and V_2 are $E_1 = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, d\}\}$ and $E_2 = \{\{e, g\}, \{f, g\}\}$, respectively.

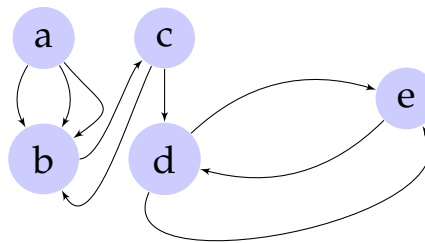
Definition (Disconnected Graph): An undirected graph $G = (V, E)$ is

disconnected if and only if V can be partitioned into at least two subsets V_1, V_2 of V such that there is no edge in E of the form (x,y) , where $x \in V_1$ and $y \in V_2$. Similarly, a graph is connected if and only if it has only one component. The number of components of $G = (V, E)$ is denoted by $\mathcal{K}(G)$.

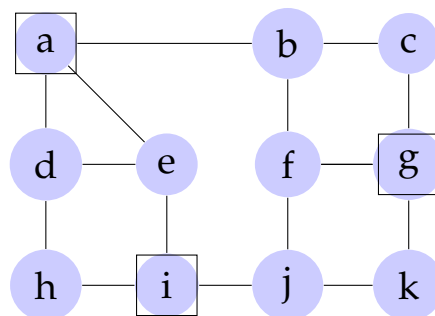
Example 4: Below are three undirected graphs with either 1 or 2 components:



Definition (Multigraph): Assume V is finite and nonempty. (V, E) determines a **multigraph** of G with vertex set V and edge set E if for some $x, y \in V$, there are two or more edges in E of the form (x, y) for a directed multigraph ($\{x, y\}$ for an undirected multigraph). Below is an example multigraph:



Example 5: Consider a model for a security system of a department store in which the cashiers are vertices and the (unblocked) aisles are edges in an undirected graph. Our goal is to place security guards at certain locations so that each cashier will have a guard or be only one aisle away from a security guard. What is the smallest number of guards to hire? Three are shown (in boxes) below. Where should others go?



Example 6: Consider the following highway system that connects seven different towns: a, b, c, d, e, f, g :

Highway	Connections
I-22	a to c passing through b
I-33	c to d then passes through b and continues to f
I-44	d to a through e
I-55	f to b passing through g
I-66	g to d

a. Construct the corresponding directed graph:

b. List paths from town g to town a (no repeat vertices).

c. What is the smallest number of highway segments that would have to be closed down to disrupt travel from town b to town d ?

- d. Is there a c - c (visit all towns once) cycle? _____
- e. Is it possible to start at some town and drive over each highway segment exactly once? You may visit any town more than once and not return where you started?

8.2 Subgraphs

Before we get into subgraphs, let's look over a couple key definitions. Let's say x and y are two vertices of a graph. A path between x and y describes a motion from x to y along edges of the graph.

Following this, a *subpath* is a portion of this path between x and y . For example, the path (C, D, E) is a subpath of (A, B, C, D, E, F) . Keep in mind that any path is its own subpath; however, we call it an *improper* subpath of itself. All other nonempty subpaths are called *proper* subpaths.

Given this definition, you could probably intuit what we mean by *subgraph*. This gets a little tricky, but for the most part you can go along with your intuition. Since graphs are comprised of two sets, vertices and edges, a subgraph G' of a graph G could involve a subset of either or both of these sets.

Definition: Let $G = (V, E)$ be a graph of any kind: directed, directed multigraph, or undirected. $G' = (V', E')$ is a subgraph of G if $\emptyset \neq V' \subseteq V$, $E' \subseteq E$, and every edge $e = \{v_1, v_2\} \in E'$ satisfies $v_1, v_2 \in V'$.

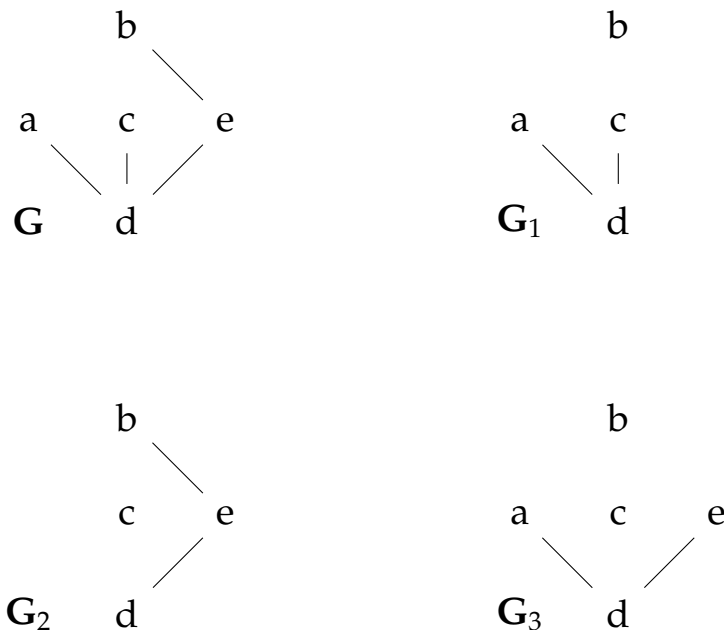
Definition (in English): A subgraph of G is created by removing zero or more vertices and all edges that include the removed vertices. Additionally, more edges may then be removed.

Two subtypes of subgraphs are an **induced** subgraph and a **spanning** subgraph:

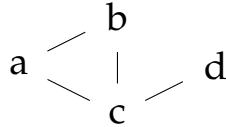
Let U be the set of vertices in a subgraph of $G = (V, E)$. If $\emptyset \neq U \subseteq V$, the subgraph of G *induced* by U , notated as $\langle U \rangle$, is the graph whose vertex set is U and whose set of edges is comprised of all edges of the form $(x, y) \in E$ or $\{x, y\} \in E$ for directed and undirected graphs, respectively. What this means is that you only remove edges which correspond to the vertices that you remove.

Let $G = (V, E)$ be a graph and $G_1 = (V_1, E_1)$ be a subgraph of G . If $V_1 = V$ and $E_1 \subseteq E$, i.e. no vertices are removed from G , only edges, then G_1 is a *spanning subgraph*.

Let G_n denote a subgraph of G . Notice some of the properties of the following graph and the corresponding subgraphs. Are some of these *spanning* graphs? How about *induced* graphs? Hint: find out what the sets of vertices and edges are for G and compare that to the sets of G_1, G_2 , and G_3 .

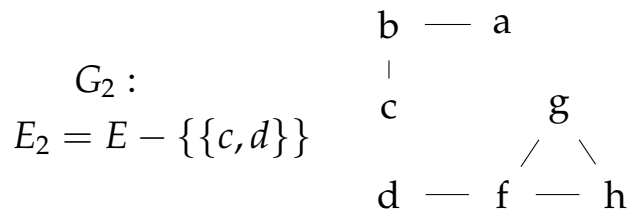
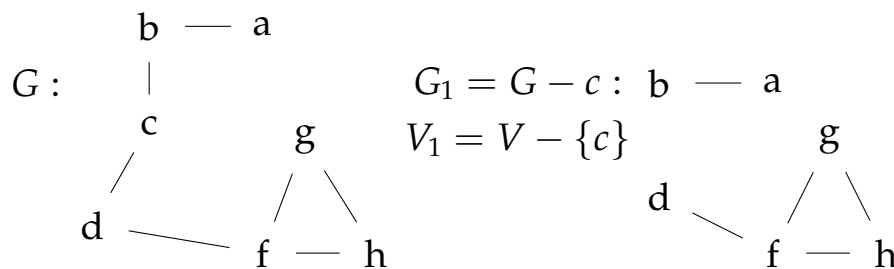


Example 1: How many spanning subgraphs does the following graph have?



Definition (Induced Subgraph): Let $G = (V, E)$ and a subgraph of G denoted by $G - v$ has the vertex set $V_1 = V - \{v\}$ and edge set $E_1 \subseteq E$ where E_1 contains all edges in E *except those incident* with vertex v . We say that $G - v$ is the subgraph **induced** by V_1 .

Example 2: Here, we show two subgraphs of the 6-vertex graph $G = (V, E)$ when either a vertex (c) or an edge ($\{c, d\}$) is removed. Is G_2 an induced subgraph?



Definition (Complete Graph): Let V be a set of n vertices. The **complete graph** on V , denoted by K_n , is a loop-free undirected graph such that for all $a, b \in V, a \neq b$, there is an edge $\{a, b\} \in E$, i.e. every vertex is connected to all others by an edge.

Example 3: Here are K_1 through K_4 . Can you draw K_5 ?

K_1 : a

K_2 : a — b

K_3 : $\begin{array}{c} a \\ / \quad \backslash \\ b \quad - \quad c \end{array}$

K_4 : $\begin{array}{ccc} a & - & b \\ | & \times & | \\ c & - & d \end{array}$

Definition: (Complement Graph): Let $G = (V, E)$ be a loop-free undirected graph where $n = |V|$. The complement of G , denoted by \overline{G} , is the subgraph of K_n consisting of all n vertices of G and all edges $e = \{v_1, v_2\} \notin E$ that satisfy $v_1, v_2 \in V$. If $G = K_n$ then $\overline{G} = \emptyset$, i.e. \overline{G} is a null graph.

Example 4: A 4-vertex graph G and its complement \overline{G} :

G : $\begin{array}{ccc} a & - & c \\ | & \backslash & \\ d & & b \end{array}$

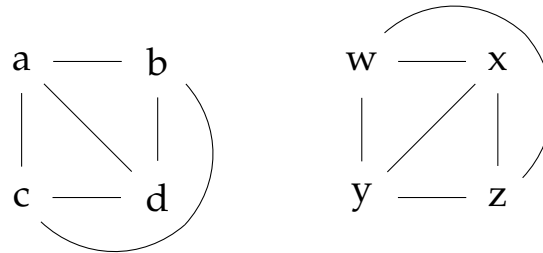
\overline{G} : $\begin{array}{ccc} a & & b \\ & / & | \\ d & - & c \end{array}$

Definition (Graph Isomorphism): Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, where G_1 and G_2 are undirected graphs. A function $f : V_1 \rightarrow V_2$ is a graph isomorphism if

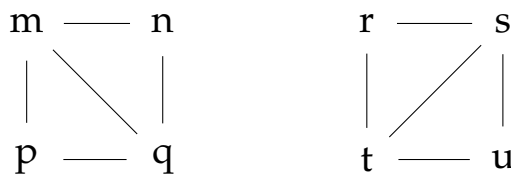
- f is 1-to-1 and onto, and
- $\forall a, b \in V_1, \{a, b\} \in E_1$ if and only if $\{f(a), f(b)\} \in E_2$.

We say G_1 and G_2 are **isomorphic** if and only if both conditions are true.

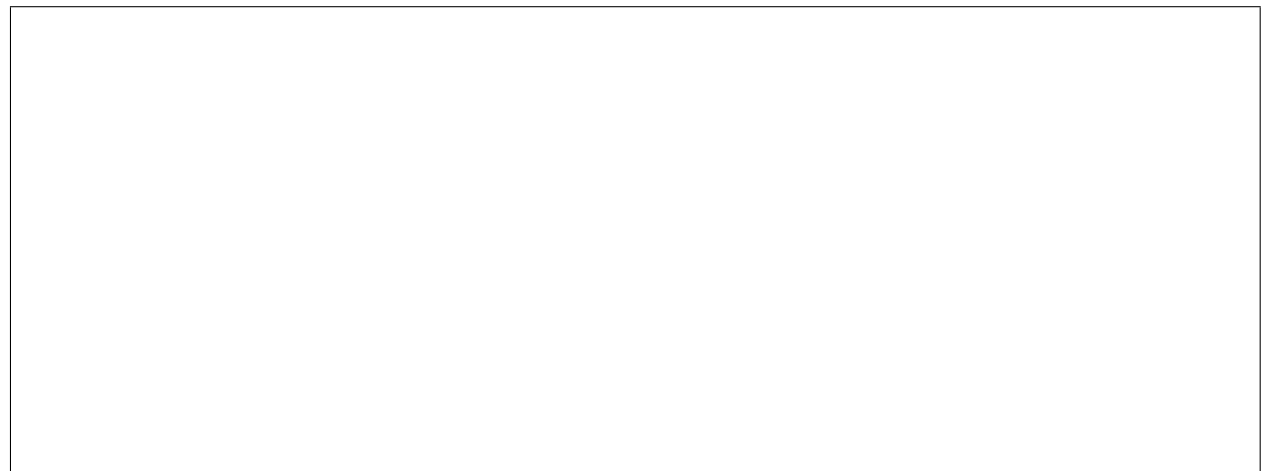
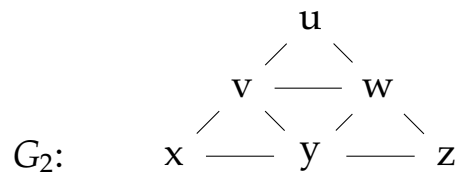
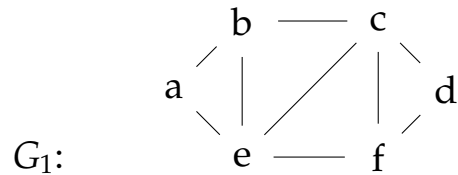
Example 5: Suppose we define $f(a) = w$, $f(b) = x$, $f(c) = y$, and $f(d) = z$. Then, $\forall \{a, b\} \in E_1, \exists \{f(a), f(b)\} \in E_2$. Hence, f is a graph isomorphism.



Example 6: For the 4-vertex graphs below, suppose $g(m) = r$, $g(n) = s$, $g(p) = t$ and $g(q) = u$. Is g a graph isomorphism? _____

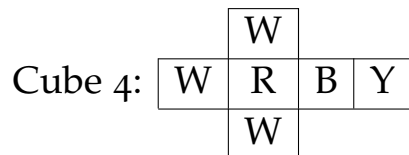
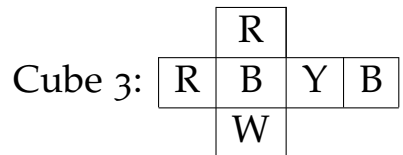
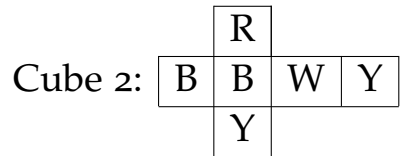
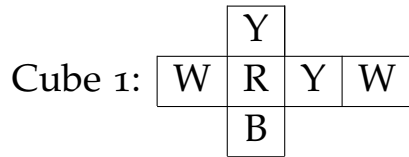


Example 7: Are the two 6-vertex graphs below isomorphic? The answer can be reached by considering the alternative question of whether or not you can find a circuit in one graph but not the other?

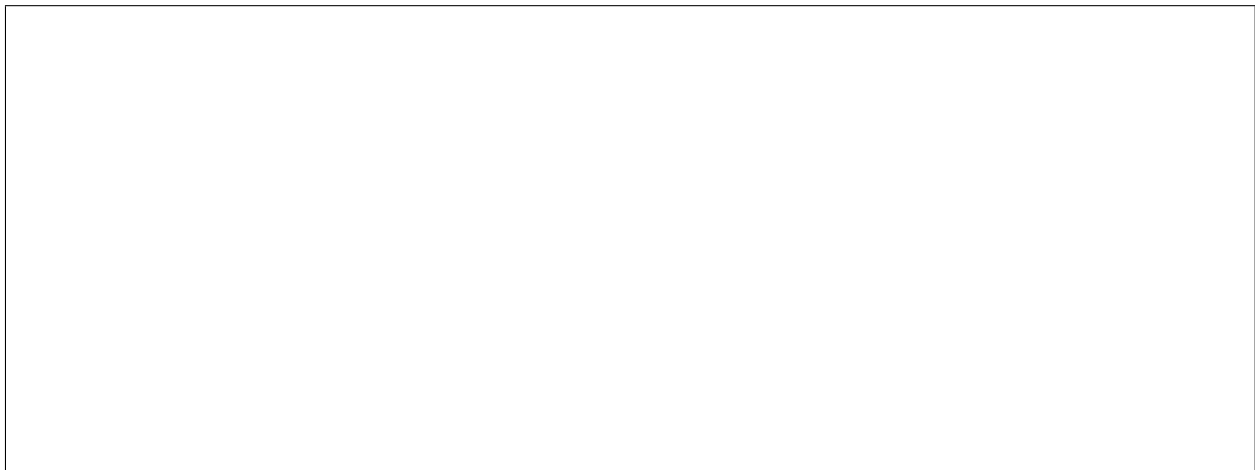


Example 8: The generation of subgraphs can be extremely helpful for solving puzzles or games such as *Instant Insanity* created for Parker Bros. in 1967 by Franz Owen Arm Bruster. In this game you have 4 cubes, each with 6 slides and each side has one of four possible colors: red (R), white (W), blue (B), and yellow (Y). The object of the game is to stack the cubes in such a way so that all four colors appear on each side of the column (of the cube stack). This is similar to Rubik's Cube.

Let's see if we can determine the proper stacking of the following cubes:



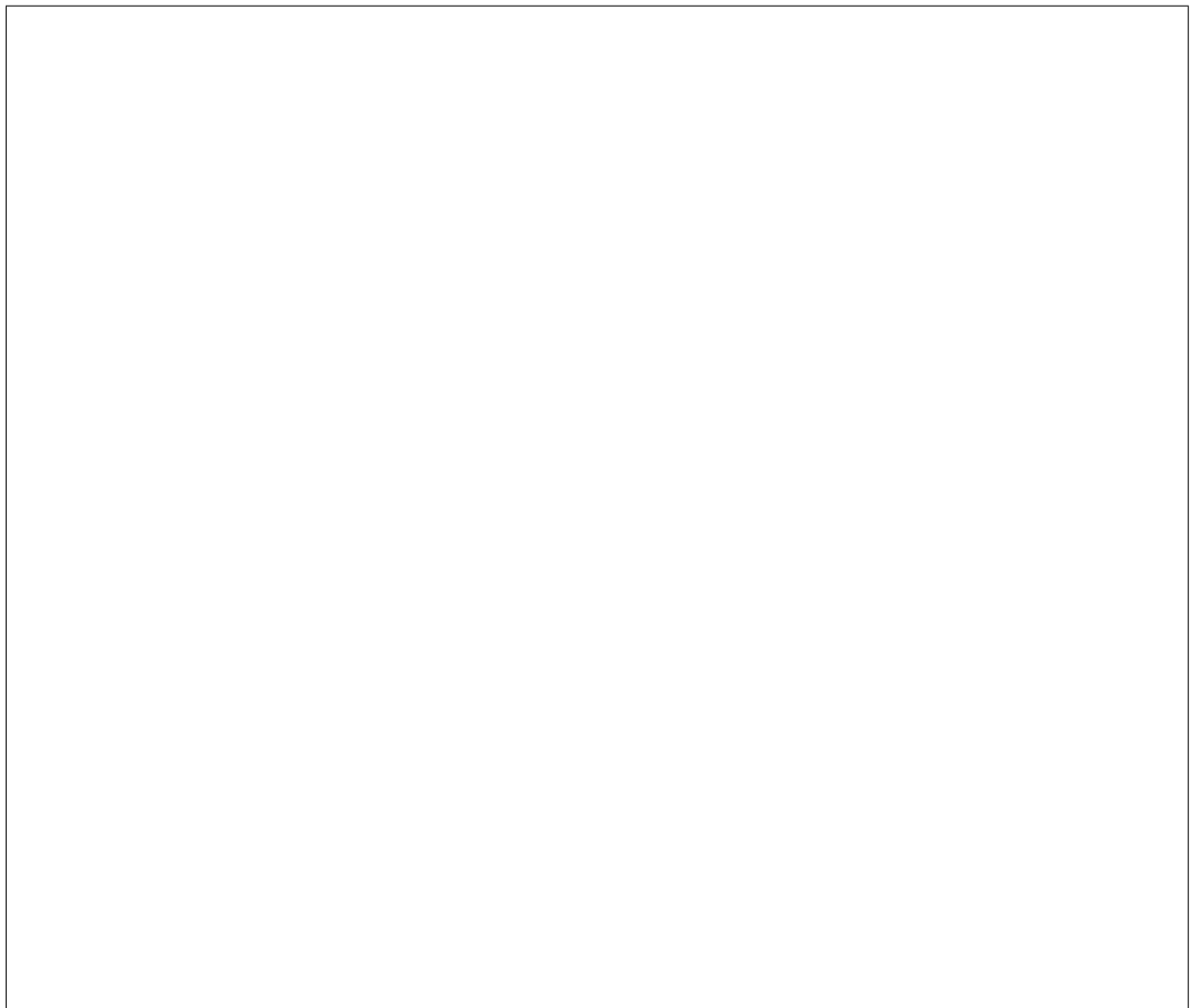
We will start by drawing a 4-vertex and 12-edge graph in which each edge represents a pair of opposite faces (sides) of a cube. Edges are labelled according to the cube that owns the corresponding faces.



At each vertex of the graph, the number of edges *incident* reflects the number of faces on the 4 cubes that have that color. Loops count for 2 faces. So, the graph reveals ____ red faces, ____ white faces, ____ blue faces, and ____ yellow faces.

With the 4 cubes stacked in a column, we examine two opposite sides of the column and seek 4 edges in the graph where each label appears once. (Each color must appear twice as an endpoint/vertex of the 4 edges.)

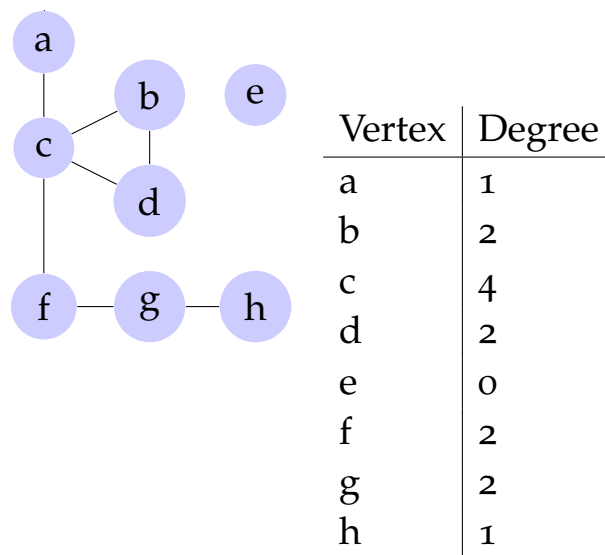
Goal: Can we find a similar set of edges representing the other pair of opposite sides of the column? If so, we have the solution. We need to produce two subgraphs, one for each pair of opposite sides of the column of cubes in which all 4 colors are showing. The two subgraphs cannot share any edges. Draw the subgraphs and the arrangement of cubes that solve the puzzle.



8.3 Vertex Degree

Definition (Vertex Degree) Let G be an undirected graph or multigraph. For each vertex v of G , the **degree** of v or $\deg(v)$ is the number of edges in G that are incident with v . A loop at vertex v is considered as 2 incident edges for v .

Example 1: The degrees of each vertex in the following 8-node graph are provided below the graph. A vertex such as h that has degree 1 is called a *pendant vertex*.

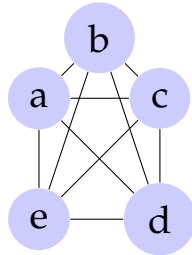


Theorem If $G = (V, E)$ is an undirected graph or multigraph then $\sum_{v \in V} \deg(v) = 2|E|$.

Corollary For any undirected graph or multigraph, the number of vertices of odd degree must be even.

Definition (Regular Graph) If $G = (V, E)$ is an undirected graph or multigraph and each vertex $v \in V$ has the same degree, we call G a **regular graph**. If $\deg(v) = k \forall v \in V$, we call G a k -regular graph.

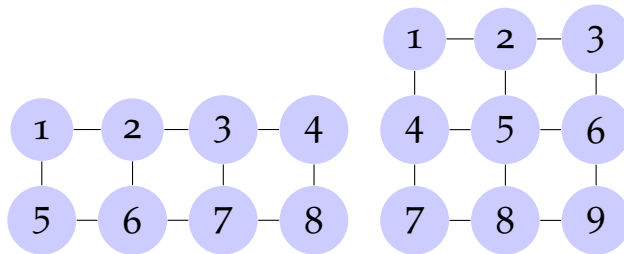
Question Can we have a 4-regular graph with 10 edges? _____



Question Can we have a 4-regular graph with 15 edges? _____. Here, we would have $2|E| = 30 = \sum \deg(v) = 4|V|$.

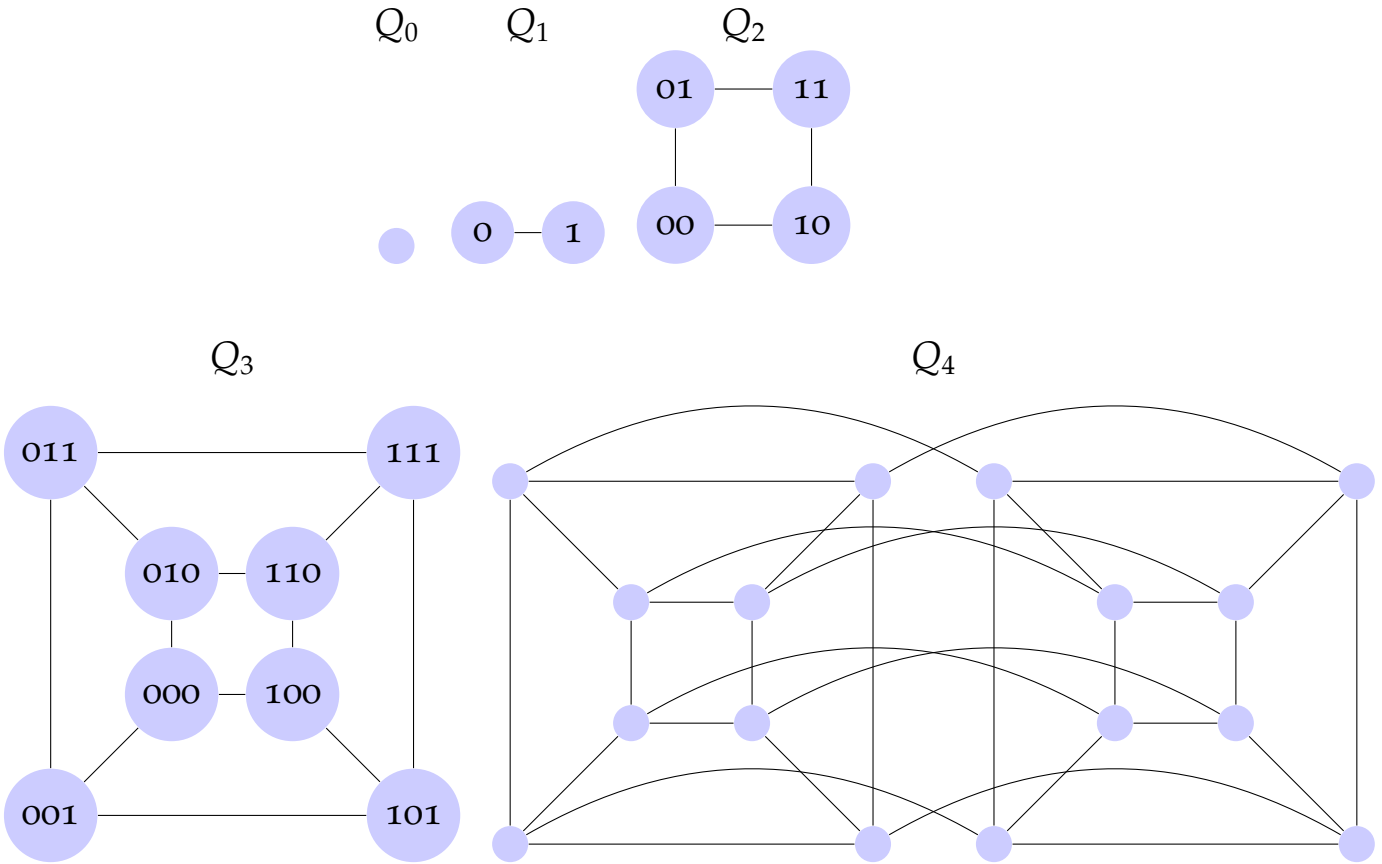
8.4 Hypercube Architecture

The hypercube processor architecture (grid) can be represented by graphs. Below are simple 2×4 (left) and 3×3 (right) grid designs:



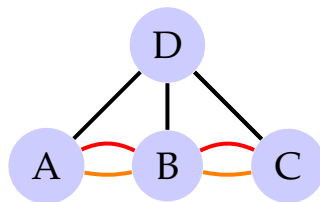
The problem with these simple (processor) grid designs is that they **do not scale**, i.e., the paths between nodes increase in length as you add more nodes (processors). We want the communication cost between any nodes in the grid to be bounded.

Definition (Hypercube): A **hypercube** is a loop-free connected and undirected graph with 2^n vertices, denoted by Q_n . Below are the first five hypercube graphs. Notice that with Q_2 , the longest path is 2 and that the binary labels of connected nodes only differ by one bit.



8.5 Famous Problems

Example 1: The Seven Bridges of Königsberg problem (18th Century) involves a city walk from a starting position that crosses every bridge once before returning to the starting position.



Question Does a circuit exist in this graph? _____. We note that $\deg(a) = \deg(c) = \deg(d) = 3$ and $\deg(b) = 5$.

Definition (Euler Circuit): Let $G = (V, E)$ be an undirected graph or multigraph with no isolated vertices. Then, G has an **Euler circuit** if \exists a circuit in G that traverses every edge in G once.

Theorem: If $G = (V, E)$ is an undirected graph or multigraph with no isolated vertices then G has an Euler circuit if and only if G is connected and every vertex in G has **even** degree.

Corollary: Under the same assumptions for G , we can construct an **Euler trail** in G if and only if G is connected and has exactly 2 vertices of odd degree. This explains why the *Seven Bridges Problem* is **not** solvable.

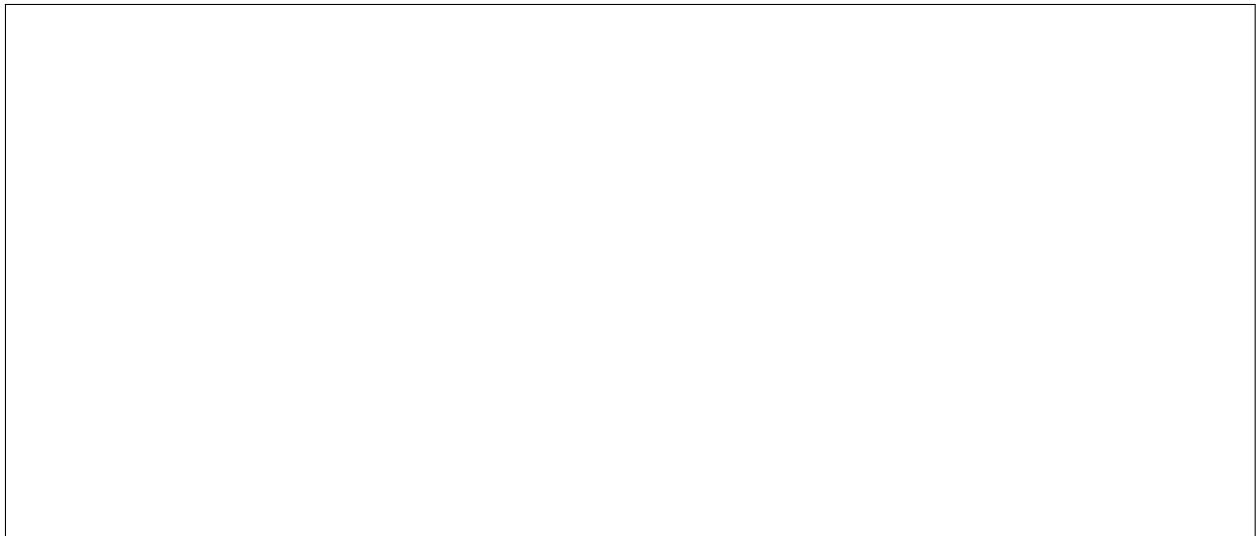
Definition (In-degree, Out-degree): Let $G = (V, E)$ be a directed graph or multigraph, for each $v \in V$:

- a. the incoming or in-degree of v is the number of edges that are incident to v (denoted by $id(v)$).

- b. the outgoing or out-degree of v is the number of edges that are incident from v (denoted by $od(v)$).

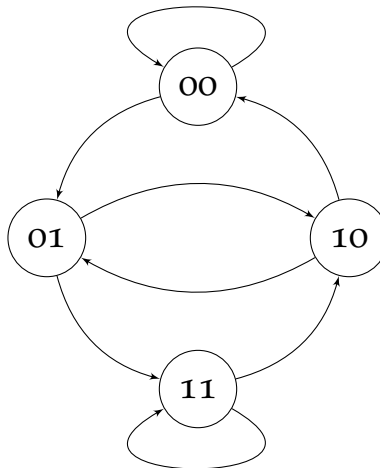
Theorem: Let $G = (V, E)$ be a directed graph or multigraph with no isolated vertices. Then G has a directed Euler circuit if and only if G is connected and $id(v) = od(v) \forall v \in V$.

Example 2: Let's consider a famous telecommunications problem posed by C.L. Liu in which an electronic drum is rotated clockwise to generate 3-digit binary codes.



Question: As the drum rotates clockwise, can we represent all 8 binary representations (000 through 111)?

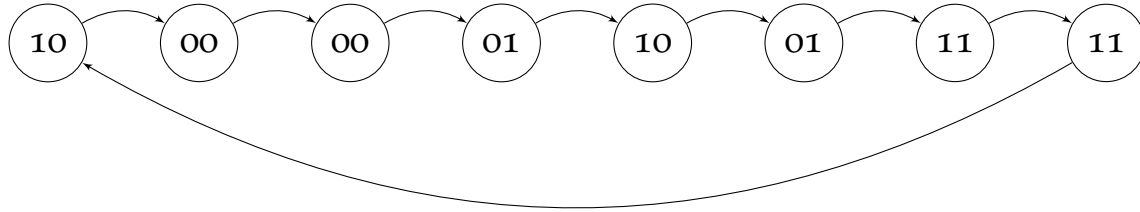
Answer: Construct a directed graph $G = (V, E)$, where $V = \{00, 01, 10, 11\}$ and a E is constructed as follows. If $b_1b_2, b_2b_3 \in V$, draw edge (b_1b_2, b_2b_3) .



So, is the graph connected? _____

Is $id(v) = od(v) \forall v \in V$? _____

By a previous theorem, \exists a directed Euler circuit:



Example 3: We can count the number of walks between any two nodes of a graph through the use of **adjacency** and **incidence** matrices. Let's assume $|E| = n$ and $|V| = k$ for a graph $G = (V, E)$. Define the adjacency matrix $A = (a_{ij})_{k \times k}$ by $a_{ij} = 1$ if $\{v_i, v_j\} \in E$, and $a_{ij} = 0$ otherwise. Define the incidence matrix $I = (b_{ij})_{n \times k}$ by $b_{ij} = 1$ if v_i is a vertex on edge j , and $b_{ij} = 0$ otherwise.

$$\text{a. } A = \begin{array}{c|ccccc} & v_1 & v_2 & v_3 & v_4 & v_5 \\ \hline v_1 & 0 & 1 & 1 & 0 & 1 \\ v_2 & 1 & 0 & 1 & 1 & 1 \\ v_3 & 1 & 1 & 0 & 1 & 1 \\ v_4 & 0 & 1 & 1 & 0 & 1 \\ v_5 & 1 & 1 & 1 & 1 & 0 \end{array}$$

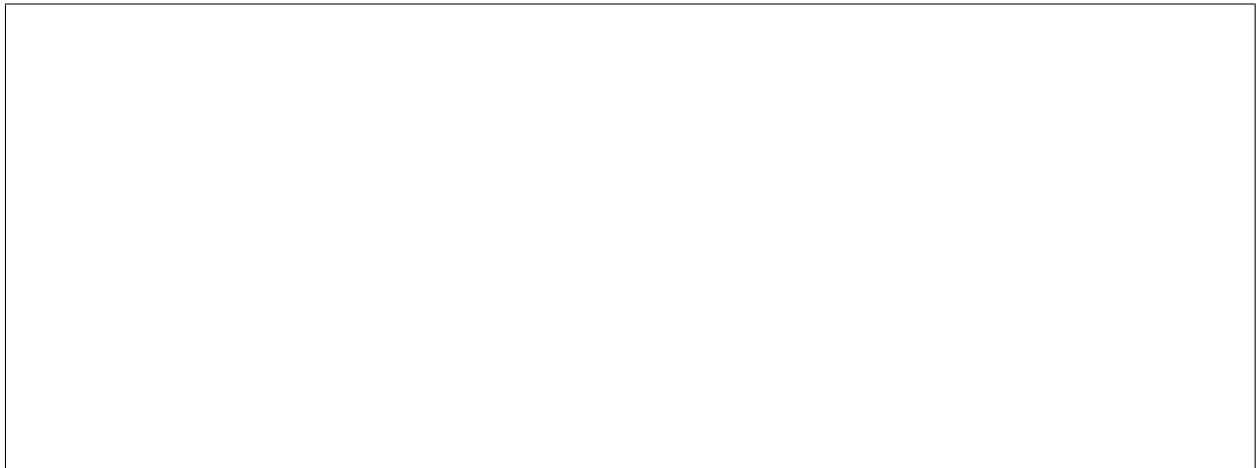
$$\text{b. } I = \begin{array}{c|cccccccccccc} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 & e_{10} & e_{11} \\ \hline v_1 & 1 & 1 & & & & & & & & & & \\ v_2 & 0 & 0 & & & & & & & & & & \\ v_3 & 1 & 0 & & & & & & & & & & \\ v_4 & 0 & 0 & & & & & & & & & & \\ v_5 & 0 & 1 & & & & & & & & & & \end{array}$$

c. Calculate $A^2 = A \times A$ (i.e., matrix multiplication). What do entries in A^2 reveal about the graph G ?

Answer: For $1 \leq i, j \leq n$, the (i, j) entry of the matrix A^2 counts the number of **distinct walks** of length 2 between vertices i and j .

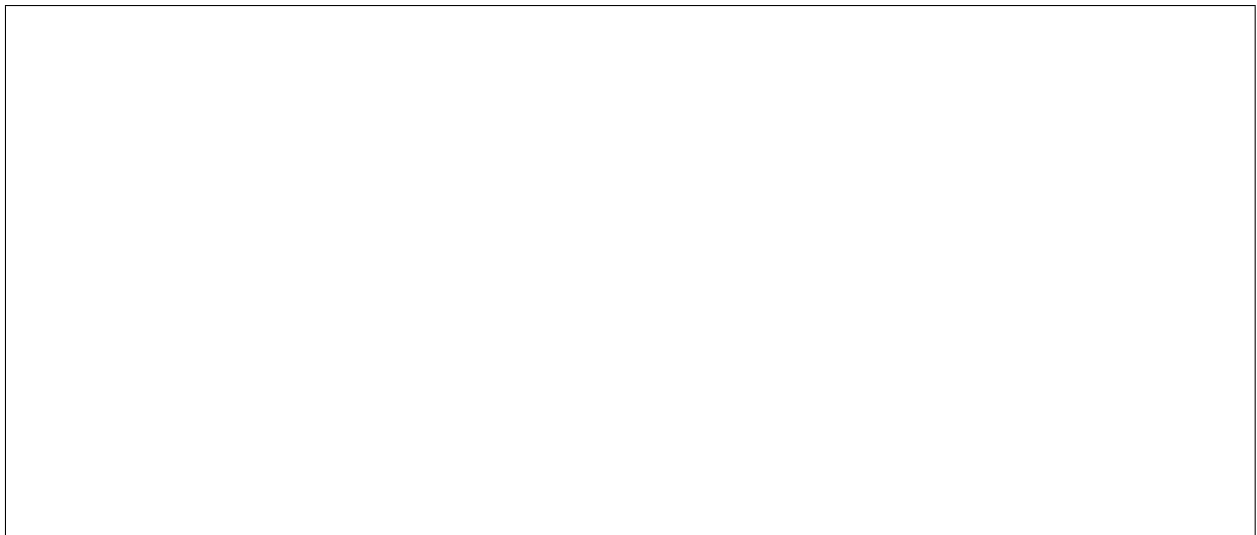
8.6 *Planar Graphs*

Definition (planar graph): A graph (or multigraph) G is **planar** if G can be drawn in the plane with edges intersecting only at the vertices. We can also say that such a graph G is an embedding of G in the plane. Let's draw a few planar and nonplanar graphs.



Notice that we can draw both a planar and nonplanar K_4 graph.

But can we embed K_5 in the plane? Let's try below. Recall that K_5 is a graph with five vertices in which every vertex is connected to every other vertex.



So, apparently K_5 is nonplanar.

8.7 Bipartite Graphs

Definition (bi-partite graph): $G = (V, E)$ is called **bi-partite** if $V = V_1 \cup V_2$ with $V_1 \cap V_2 = \emptyset$ and every edge of G is of the form $\{a, b\}$ with $a \in V_1$ and $b \in V_2$. In other words, G_4 is bi-partite if the vertices are divided into two sets V_1 and V_2 and each edge goes from a vertex in V_1 to a vertex in V_2 . The two sets V_1 and V_2 cannot contain the same vertex, but when combined must contain every vertex of the graph G .

Q_n is bi-partite $\forall n \geq 1$. Let's draw the first three below:

Q_1 :

$$V_1 = \{0\}$$

$$V_2 = \{1\}$$

Q_2 :

$$V_1 = \{00, 11\}$$

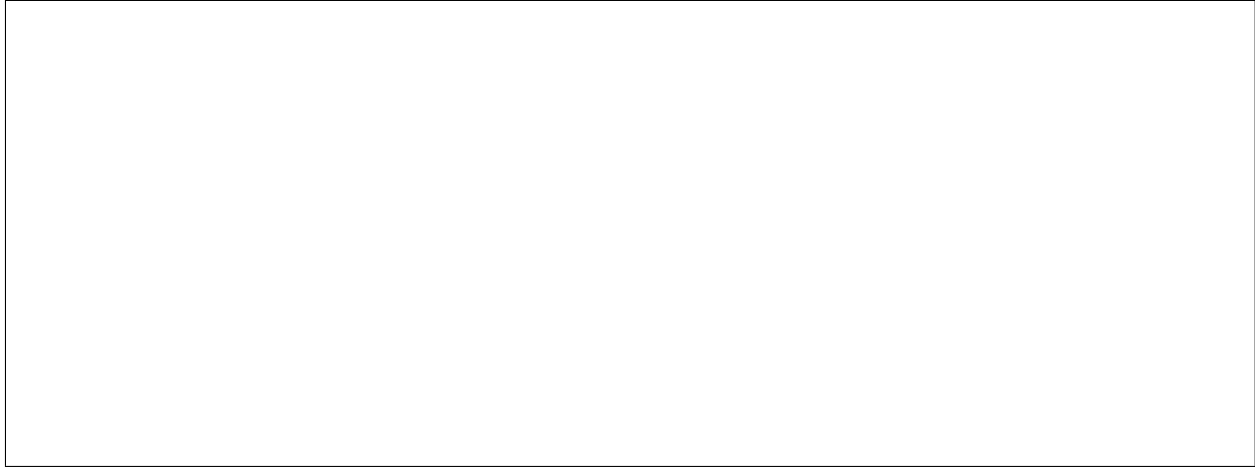
$$V_2 = \{01, 10\}$$

Q_3 :

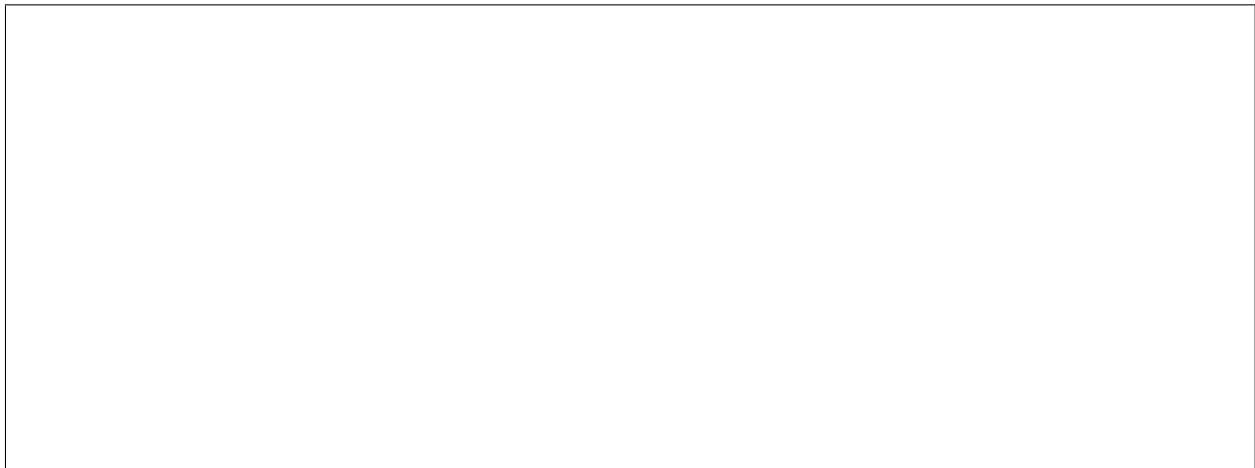
$$V_1 = \{000, 011, 101, 110\}$$

$$V_2 = \{001, 010, 100, 111\}$$

Example 1: Consider the following graph with $V_1 = \{a, b\}$ and $V_2 = \{c, d, e\}$ and determine whether or not it is bi-partite. If you add the edges $\{b, d\}$ and $\{b, c\}$, is the graph complete?



Example 2: Suppose we wanted to hook up three houses to heating, water, and electricity utilities. Can we give each house all three utilities without overlapping lines? Let $V_1 = \{h_1, h_2, h_3\}$ and $V_2 = \{u_1, u_2, u_3\}$.



Notice that we cannot connect h_2 to u_2 without crossing lines. This graph is a $K_{3,3}$ nonplanar graph.

8.8 Elementary Subdivision and Homeomorphic Graphs

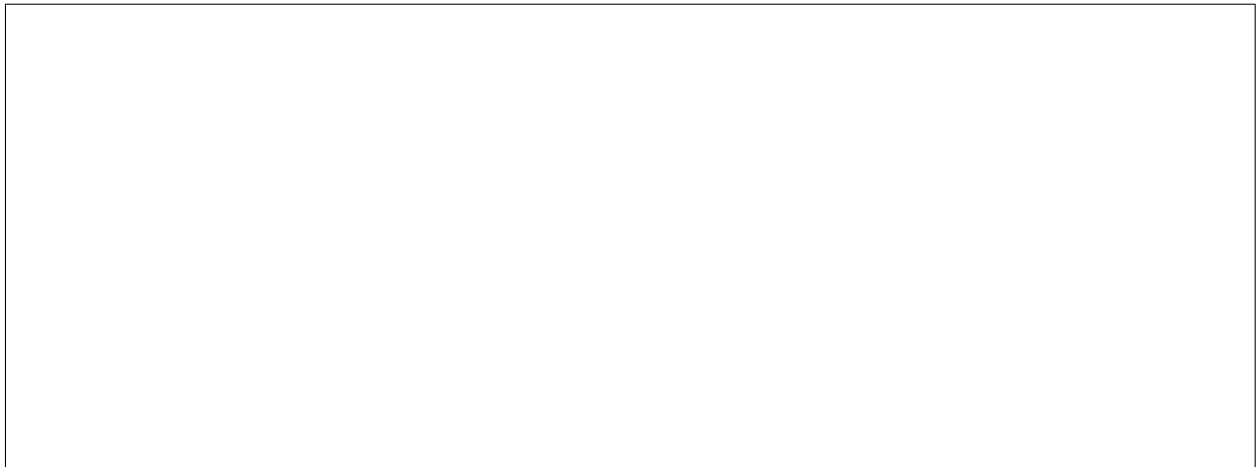
Definition: If $G = (V, E)$ is loop-free and undirected with $E \neq \emptyset$ then an **elementary subdivision** of G is a graph obtained from G by removing an edge $e = \{u, w\}$ and adding new edges $\{u, v\}$ and $\{v, w\}$ to $G - e$, where the new vertex $v \notin V$.

Definition (homeomorphic graph): Suppose G_1 and G_2 are two loop-free, undirected graphs with $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$. We say that G_1 and G_2 are **homeomorphic** if they are isomorphic or can be obtained from the same loop-free undirected graph H by a sequence of elementary subdivisions.

Let's draw three homeomorphic graphs below.

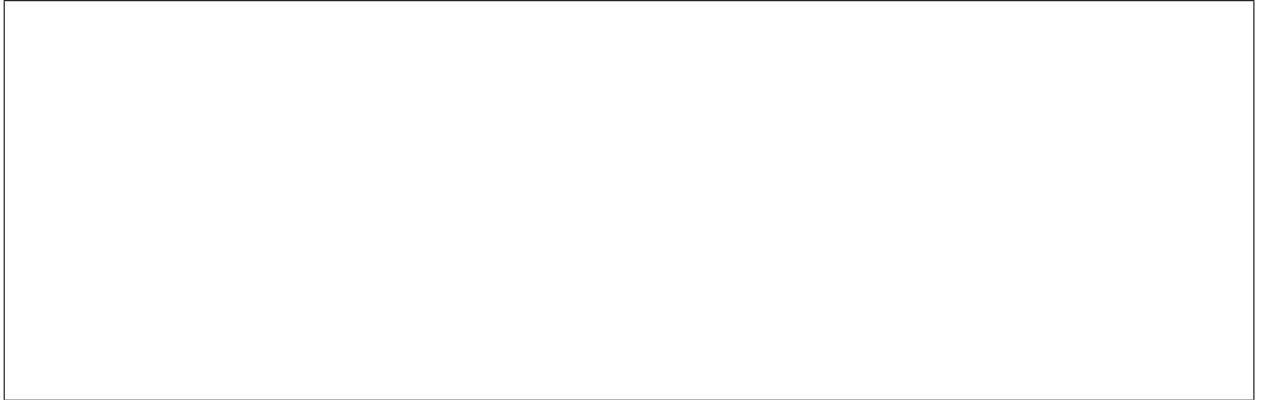


Theorem (Kuratowski's): A graph is nonplanar if and only if it contains a subgraph that is homeomorphic to either K_5 or $K_{3,3}$ (circa 1930). A classic example is the Petersen graph that we will draw below.



Example 1: We will create a subgraph of the Petersen graph that is homeomorphic to $K_{3,3}$ to prove that it is indeed nonplanar.

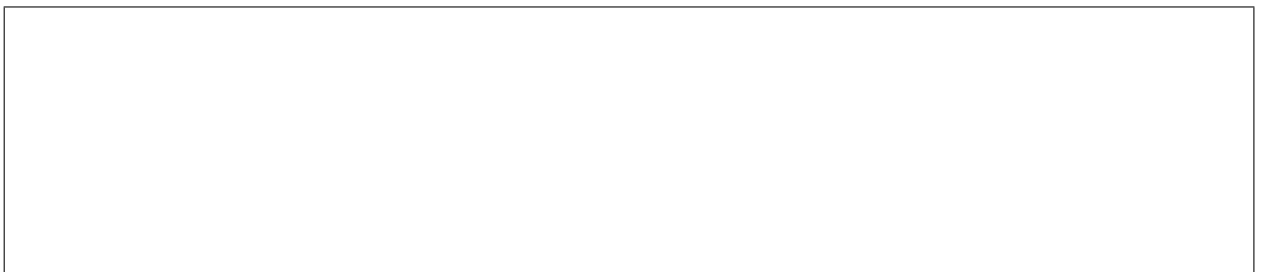
(1) Begin with a bipartite subgraph $V_1 = \{j, a, d\}$ & $V_2 = \{e, f, b\}$.



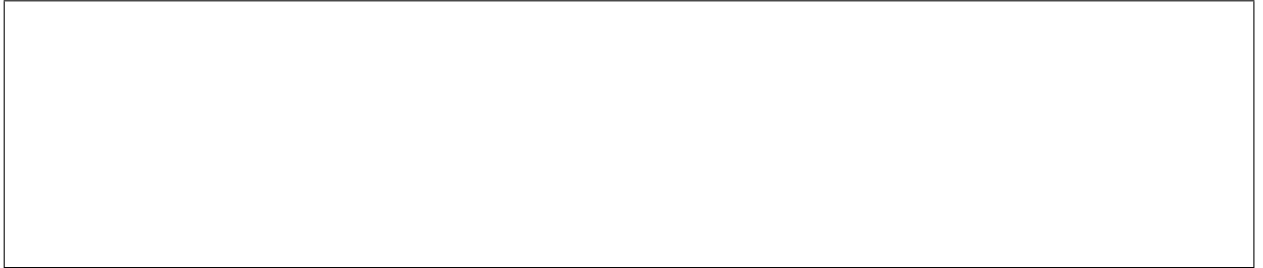
(2) Break $\{b, d\}$ and add $\{d, c\}, \{c, b\}$.



(3) Break $\{b, j\}$ and add $\{b, g\}, \{g, j\}$.



(4) Break $\{f, j\}$ and add $\{f, h\}, \{h, j\}$.

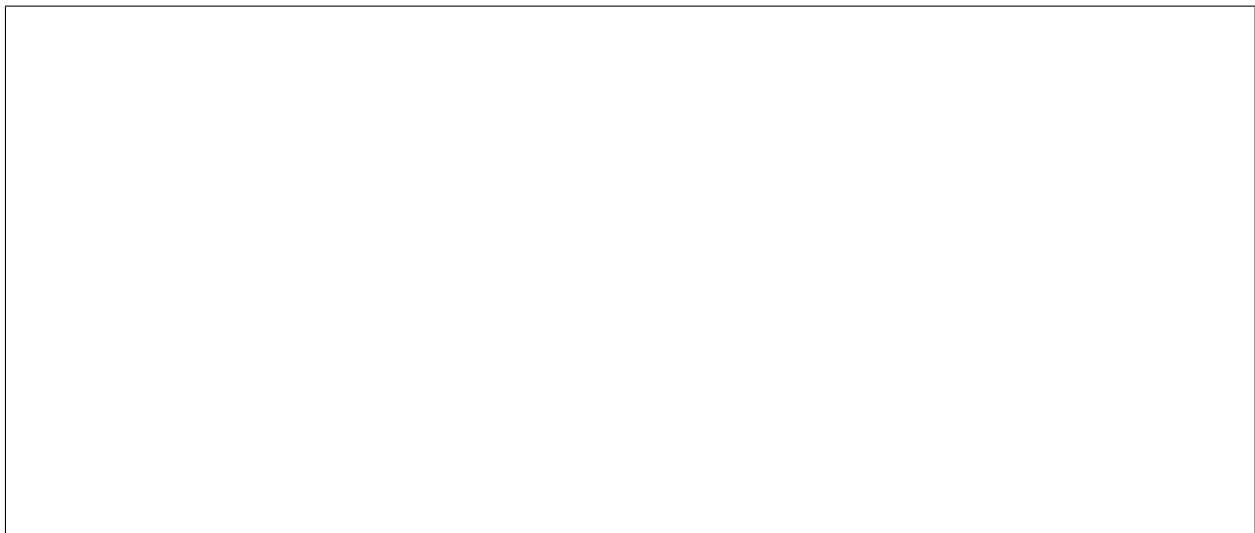


(5) Break $\{d, f\}$ and add $\{d, i\}, \{i, f\}, \{g, i\}, \{h, c\}$.

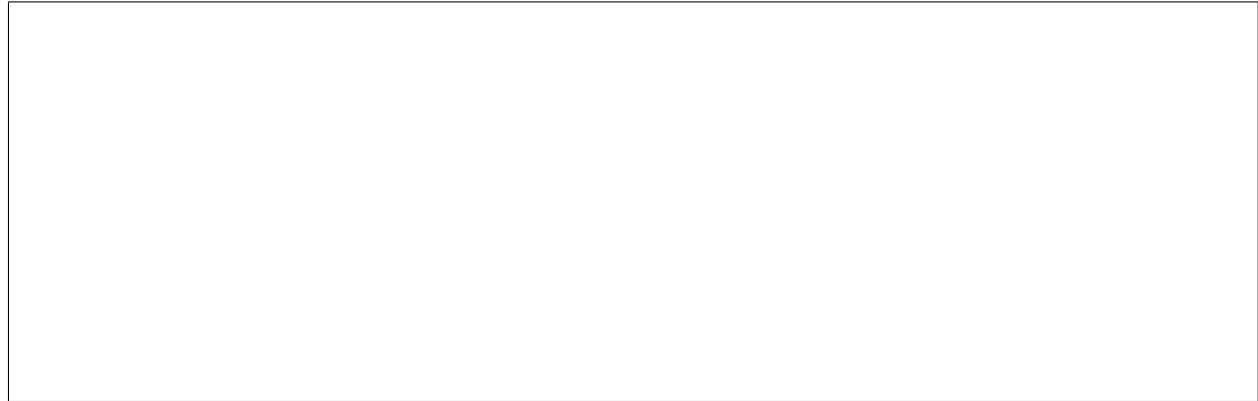


Our final graph (although it may be a bit disguised) is the Petersen graph. So, by Kuratowski's Theorem, we conclude that the Petersen graph is non-planar since it has a subgraph homeomorphic to $K_{3,3}$.

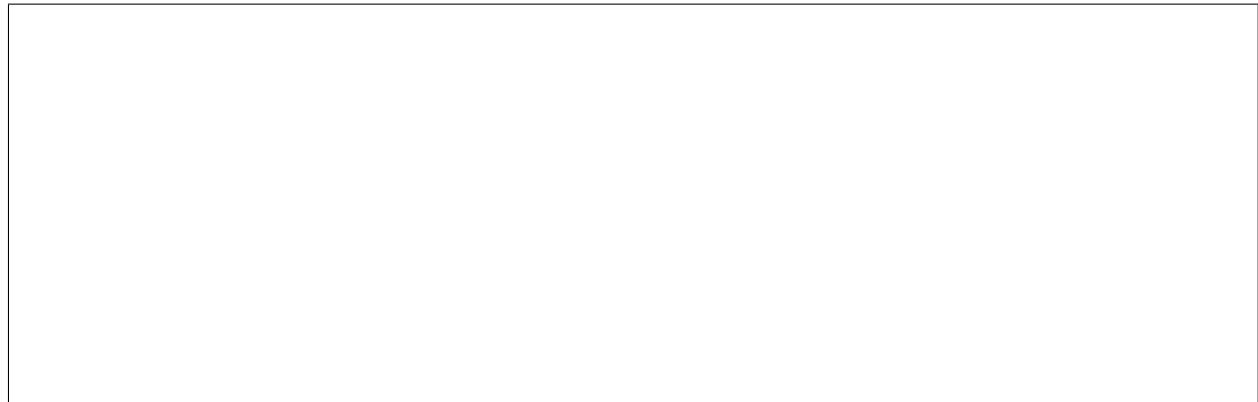
Example 2: Let's take a 3-regular graph G that is isomorphic to Q_3 and then draw its 4-regular complement (\overline{G}) .



We can find a subgraph of \overline{G} say H that is homeomorphic to K_5 and conclude that \overline{G} is nonplanar.



Euler revealed that you can count the number of *regions* determined by a planar connected graph (or multigraph) and that this number is consistent for all planar embeddings of the graph.



8.9 Euler's Theorem

Theorem (Euler's): Let $G = (V, E)$ be a connected, planar graph or multigraph with $|V| = v$ and $|E| = e$. Also, let r be the number of regions in the plane determined by a planar embedding of G and one of the infinite regions. Then,

$$v - e + r = 2 .$$

Definition (Degree of Region): The **degree** of the region R in a planar embedding of a planar graph or multigraph is the number of edges traversed in a shortest closed walk about the edges on boundary of R .

Example 1: The sum of degrees is conserved for all planar embeddings of a planar graph. Consider the 4-region case below:

Region	Degree of Region
R_1	5
R_2	3
R_3	3
R_4	7
R_5	4
R_6	3
R_7	5
R_8	6

Corollary: Let $G = (V, E)$ be a loop-free connected, undirected planar graph with $|V| = v$, $|E| = e > 2$ and r regions. Then,

$$3r \leq 2e \text{ and } e \leq 3v - 6 .$$

Example 2: K_5 is a loop-free connected graph with **10** edges and **5** vertices. That is, $3v - 6 = 3(5) - 6 = 15 - 6 = 9$ but $e = 10 \not\leq 9$ so K_5 is **not** planar.

Dual graphs:

The following is the process of constructing a dual graph (G^d) for a given **planar embedding** $G = (V, E)$. Let $V = \{a, b, c, d, e, f\}$.

- 1) Place a point (vertex) inside each region (include infinite region).
- 2) For each edge shared by two regions, draw an edge connecting the *inside* vertices.
- 3) For an edge traversed twice in a closed walk about the edge of a region, draw a loop at the vertex for this region.

Example 3: A loop in G can produce a pendant vertex in G^d if the loop contains no other vertex/edge in G . The degree of a vertex in G^d is the number of edges on boundary of a closed walk about the region on G that contains the vertex.



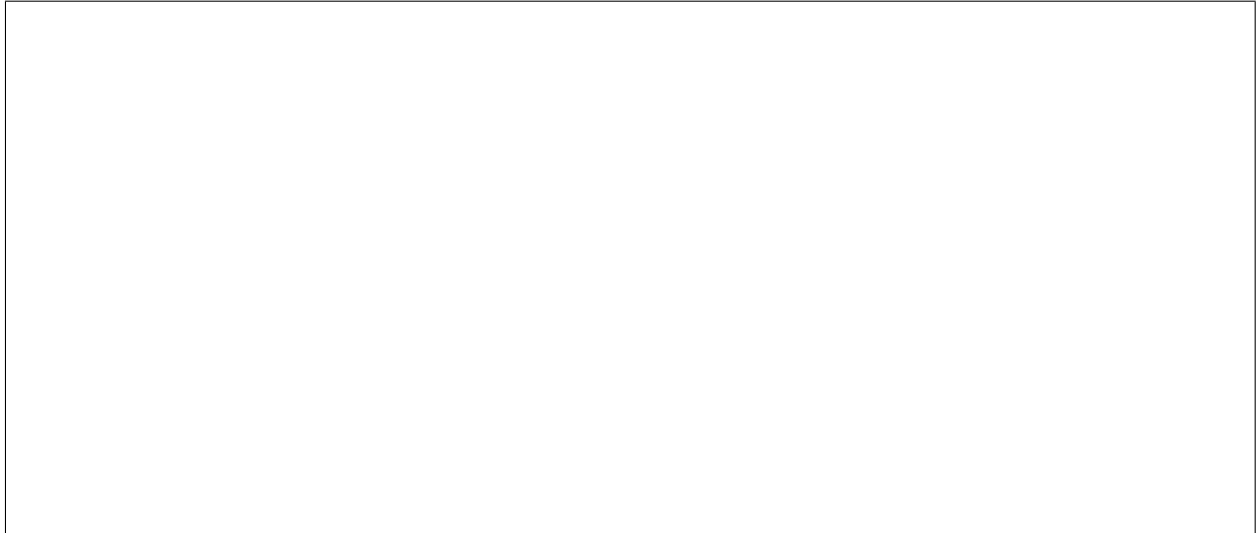
Definition (cut-set) : Let $G = (V, E)$ be an undirected graph or multi-graph. A subset E' of E is called a **cut-set** of G if by removing the edges in E' from G , we have $K(G) < K(G')$ where $G' = (V, E - E')$ and $K(\cdot)$ is the number of components.

But, when we remove from E any proper subset E'' of E' we have $K(G) = K(G'')$ for $G'' = (V, E - E'')$. So, the cut-set is a minimal disconnecting set of edges for a given connected graph.

Example 4: Here, we illustrate a *bridge* or a 1-edge cut-set.

cut-sets of G'	$K(G')$
$\{a, b\}, \{a, c\}$	2
$\{a, b\}, \{c, d\}$	2
$\{e, h\}, \{f, h\}, \{g, h\}$	2
$\{d, f\}$	2

Example 5: Consider a 5-region map (and ignore the infinite region) and suppose we want to color the five regions so that two countries/states that share a common border are colored differently. Given $G = (V, E)$ construct G^d so that any two connected vertices are colored differently (this is the infamous **Four-Color Theorem** for planar graphs).



Example 6: Consider a 9-switching network that controls a light source. Suppose we want to construct a *dual* network so that the light in this new network will be on whenever the light in the original network would be off. We start by creating a (planar) graph G whereby each switch is represented by an edge and connected edges reflect connected switches. We also add an edge between the original terminals of the network. The graph G' is then created from G whereby each vertex of G' represents a region of G . Finally, we construct G'^d and label edges in G'^d in a way that reflects the edges traversed in G for a given region. The desired network is obtained by closing all the switches in G'^d that would be open in G .



9 HAMILTONIAN PATHS AND CYCLES

9.1 *Definitions*

Hamiltonian components were named after the individual who popularized them - the Irish mathematician William Rowan Hamilton. His claim to fame is the *icosian* game. A game where the player's goal is to find a cycle along the edges of a dodecahedron such that every vertex is visited only once and the player ends the path where they started the path. This describes the **Hamiltonian cycle** (sometimes called the Hamiltonian circuit).

Definition (Hamiltonian cycle): A **Hamiltonian cycle** is a cycle that visits each vertex of a graph only once (except for the vertex that is both the start and end, which is visited twice) - a Hamiltonian graph is a graph or multi-graph with 3 or more vertices that has a Hamiltonian cycle.

Definition (Hamiltonian path): A **Hamiltonian path** is a path in a graph or multigraph that contains each vertex (only once). It does not have to return to the beginning vertex, it only has to reach every vertex once.

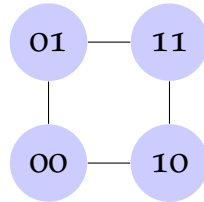
Observation:

There are no formal conditions that will guarantee that a graph will contain a Hamiltonian cycle or define a Hamiltonian path, thus proving the existence of a Hamiltonian cycle and the its Hamiltonian path is a prime example of an *NP-Complete* problem (covered in COSC 312).

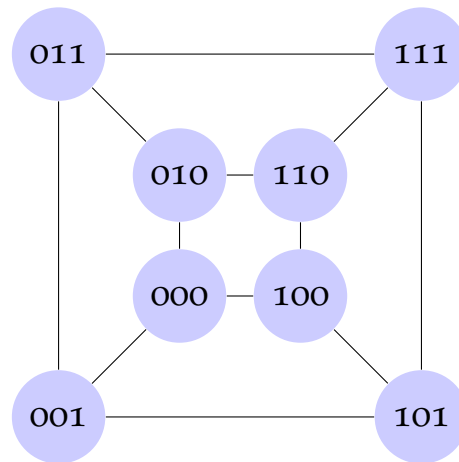
Fun Facts:

- If a graph has a Hamiltonian cycle, you can delete one of the edges in the cycle and obtain a Hamiltonian path.
- A graph can have a Hamiltonian path but not a Hamiltonian cycle.
- If a graph has a Hamiltonian cycle, then it must be connected.

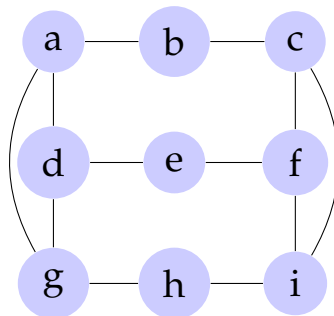
Example 1: Does the graph below contain a Hamiltonian cycle? _____



Example 2: Does the graph below contain a Hamiltonian cycle? _____



Example 3: Does the graph below contain a Hamiltonian cycle?



9.2 Properties

Properties of Graphs with Hamiltonian cycles (assume V is the vertex set):

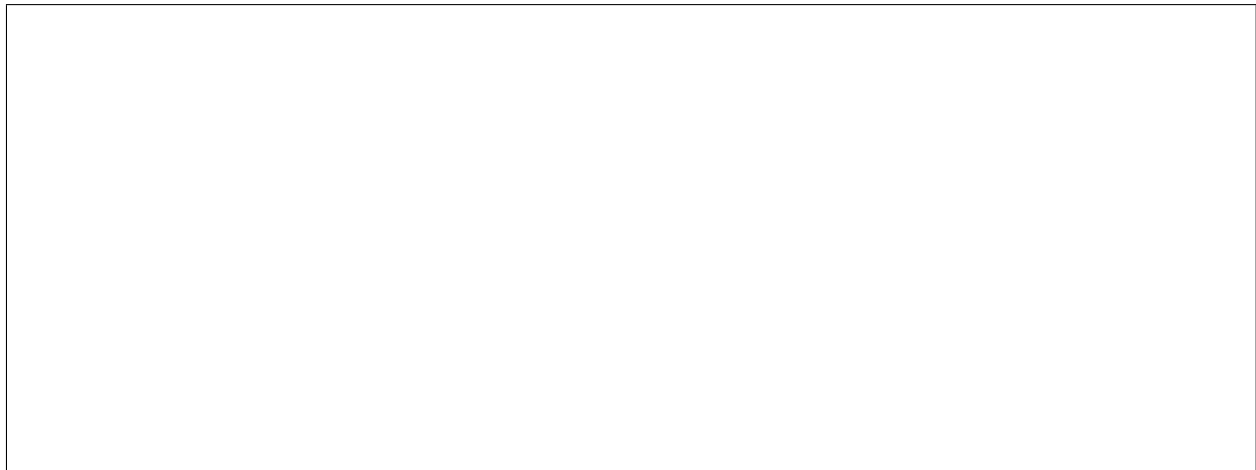
- If a graph has a Hamiltonian cycle, then for all $v \in V$, $\text{degree}(v) \geq 2$.
- If $a \in V$ and $\text{degree}(a) = 2$, then the two edges that are incident with vertex a must appear in **every** Hamiltonian cycle of the graph.

- If $a \in V$ and $\text{degree}(a) > 2$ and you pass through vertex a when constructing a Hamiltonian cycle, any unused edges incident with a can be removed from further consideration.
- It is impossible to create a Hamiltonian cycle for the subgraph of a graph unless the subgraph contains all the vertices of the original graph.

Example 4: Let's draw a connected graph $G = (V, E)$ with

$$V = \{a, b, c, d, e, f, g, h, i, j\}$$

and $|V| = 10$. Can we determine if the graph has a Hamiltonian path?



Bi-Partite Labeling Strategy: We can relabel the vertices in the above graph as a series of alternating letters or numbers where no adjacent vertex has the same label (suppose we use x and y) and obtain a *bi-partite* graph.



Does the bi-partite graph have a Hamiltonian path? _____

Does this graph have an odd cycle? _____

A bi-partite graph cannot have a cycle of odd length (that is, a closed path with an odd number of edges). In the above graph, we should have 5 x 's and 5 y 's but we end up with 4 x 's and 6 y 's, thus the graph cannot have a Hamiltonian path or cycle.

Observation: If you are given a connected graph labeled in a bi-partite fashion and it has an odd cycle then it does **NOT** contain a Hamiltonian path and thus no Hamiltonian cycle.

Note: You can use relabeling to prove a graph **does not** contain a Hamiltonian path, but you cannot use relabeling to prove that it **does** contain a Hamiltonian path. Bi-Partite graphs without odd cycles are not guaranteed to contain Hamiltonian paths.

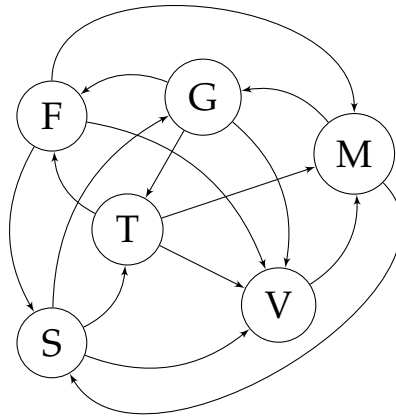
9.3 Tournament Graphs

Theorem (Tournament): Let K_n^+ be a *complete* directed graph. So K_n^+ has n vertices and for each distinct pair of vertices x and y exactly one of the edges (x, y) or (y, x) is in K_n^+ . We call K_n^+ a **tournament** and it is guaranteed to contain a directed Hamiltonian path.

Example 5: Example of a tournament based on SEC-East with Kentucky on probation (sorry wildcat fans).

SEC-East Championship Dilemma

Record	Teams: G, F, M, S, T, V
3-2 F	Beat V, S and M. Lost to T and G
3-2 G	Beat F, V and T. Lost to M and S
2-3 M	Beat G and S. Lost to F, T and V
3-2 S	Beat G, T and V. Lost to M and F
3-2 T	Beat F, M and V. Lost to G and S.
1-4 V	Beat M. Lost to F, G, S and T.



Knowing what we have listed above, is there a way to list the teams in such a way that the current team has beaten the next? In other words, can we construct a Hamiltonian path on the directed graph above?

If we can, how many Hamiltonian Paths begin with G? F? T? or S?

9.4 *Useful Theorems and their Corollaries*

Theorem (Paths): Let $G = (V, E)$ be a loop-free graph with $|V| = n \geq 2$ where n is an integer value. If $\text{degree}(x) + \text{degree}(y) \geq n - 1$ for all $x, y \in V$ where $x \neq y$ then G must have a Hamiltonian path.

Corollary: Again, let $G = (V, E)$ be a loop-free graph with $|V| = n \geq 2$ where n is an integer value. If $\text{degree}(v) \geq (n - 1)/2$ for all $v \in V$, then G has a Hamiltonian path.

Theorem (Cycles): (Ore, 1960) Let $G = (V, E)$ be a loop free *undirected* graph with $|V| = n \geq 3$ where the value n is an integer. If $\text{degree}(x) + \text{degree}(y) \geq n$ for all *non-adjacent* $x, y \in V$ then G must have a Hamiltonian cycle.

Corollaries: Again, let $G = (V, E)$ be a loop free *undirected* graph with $|V| = n \geq 3$ where n is an integer value.

1. If $\text{degree}(v) \geq n/2$ for all $v \in V$, then G has a Hamiltonian cycle.
2. If $|E| \geq \binom{n-1}{2} + 2$ then G has a Hamiltonian cycle.

9.5 *Graph Coloring*

Problem – For the storage of chemical compounds in a company's warehouse, some acids and bases cannot be near each other. Suppose the warehouse is partitioned into separate areas so incompatible chemicals can be separated. How many compartments are need?

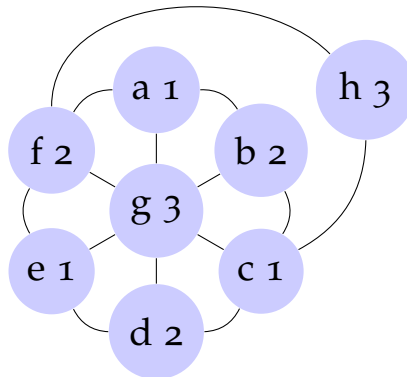
Model: For 25 chemical compounds define $V = \{C_1, C_2, \dots, C_{25}\}$. For all $1 \leq i < j \leq 25$, draw edge $\{C_i, C_j\}$ if C_i and C_j must be stored separately. Construct $G = (V, E)$ as an undirected graph.

Definition (Coloring): If $G = (V, E)$, a proper coloring of G is a color/labeling of the vertices of G so that if $\{a, b\} \in E$, then a and b are colored/labeled differently. The Chromatic number of G , denoted $\chi(G)$ is the minimum number of colors needed to properly cover G .

Some history:

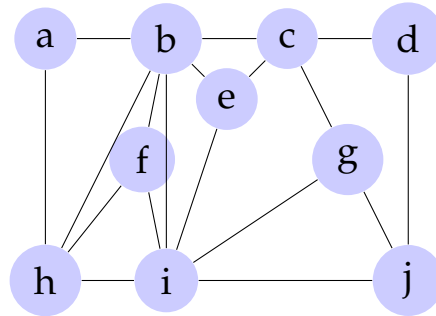
- Determining $\chi(G)$ was studied around 1850 by Francis Guthrie and later by Augustine DeMorgan in 1852.
- Determining the smallest number of colors needed to color a planar graph was called the "Four Color Problem." It was claimed to be answered by Arthur Cayley in 1879.
- Sir Alfred Kempe provided a formal proof, but had an error discovered by Percy Heawood (1861-1955). The proof stood for a decade.
- In 1976, Professor Ken Appel and Wolfgang Haken confirmed $\chi(G) = 4$ for planar graphs by computer.

Example 1: Find a subgraph isomorphic to K_n to determine $\chi(G)$.



We see that the subgraph using only vertices a , b , and g is isomorphic to K_3 and it is easy to show that $\forall n \geq 1$, $\chi(K_n) = n$. Hence, $\chi(G) = 3$ for the 8-vertex graph G above. If G is the Petersen graph, then $\chi(G) = 3$ as well.

Example 2: Suppose we wanted to determine $\chi(G)$ for the 10-vertex graph G below.



Notice that for $U = \{b, f, h, i\}$, the induced subgraph $\langle U \rangle$ is isomorphic to K_4 for $\chi(G) \geq \chi(K_4) = 4$. The following coloring will suffice:

red	green	white	blue
b, j	a, d, i	e, h, g	c, f

Is there a formal method to determine $\chi(G)$?

Assume $G = (V, E)$ is undirected and λ colors are available for coloring the vertices in V .

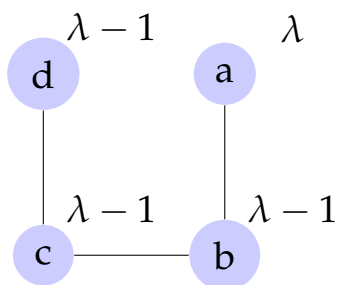
Definition (Chromatic Polynomial): $P(G, \lambda)$ is the chromatic polynomial of G that indicates how many different ways G can be properly colored using at most λ colors. A coloring can be thought of as a function $f : V \rightarrow \{1, 2, \dots, \lambda\}$ where $f(u) \neq f(v)$ for adjacent vertices $u, v \in V$.

Example 1: For $G = (V, E)$, $|V| = n, E = \emptyset$ (only isolated vertices), $P(G, \lambda) = \lambda^n$.

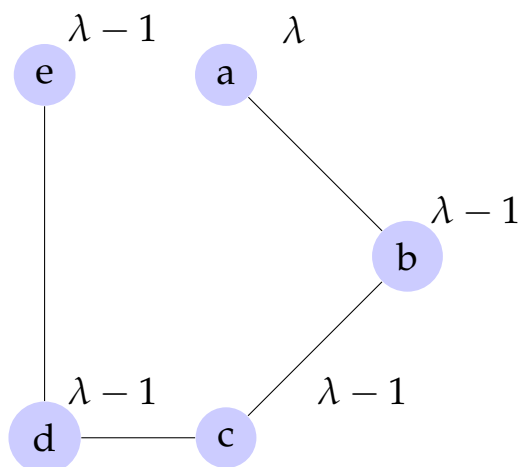
Example 2: For $G = K_n$, $P(G, \lambda) = (\lambda)(\lambda - 1)(\lambda - 2) \cdots (\lambda - n + 1) \equiv \lambda^{(n)}$.

Example 3: If $\lambda < \chi(G)$, then $P(G, \lambda) = \underline{\hspace{2cm}}$.

Example 4: Determine $P(G, \lambda)$ for the 4-vertex graph below.

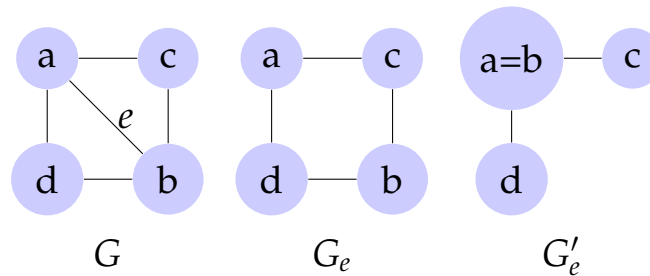


Example 5: Determine $P(G, \lambda)$ for the 5-vertex graph below.



Upshot: If G is defined by a path on n vertices, then $P(G, \lambda) = (\lambda)(\lambda - 1)^{n-1}$. If G has k components G_1, G_2, \dots, G_k , then $P(G, \lambda) = P(G_1, \lambda) \times P(G_2, \lambda) \times \dots \times P(G_k, \lambda)$.

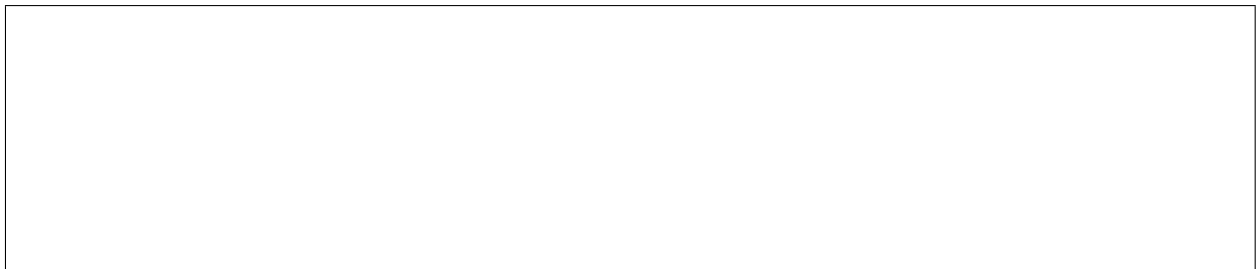
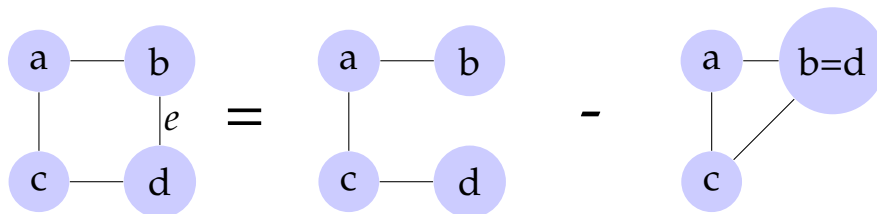
Definition (G_e): Let $G = (V, E)$ be an undirected connected graph and for $e = \{a, b\} \in E$, let G_e be the subgraph of G obtained by deleting e from G without removing vertices a and b . Now define G'_e as another subgraph of G obtained by coalescing (merging) vertices a and b from G_e .



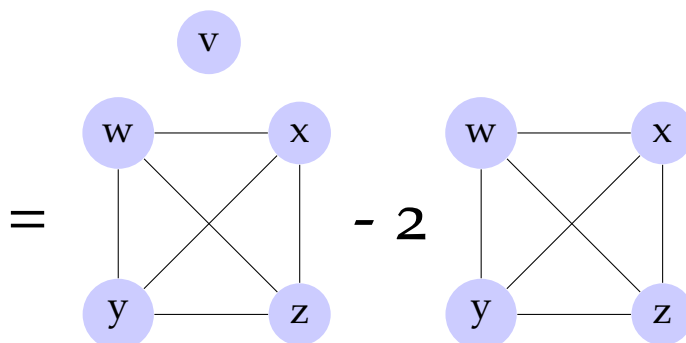
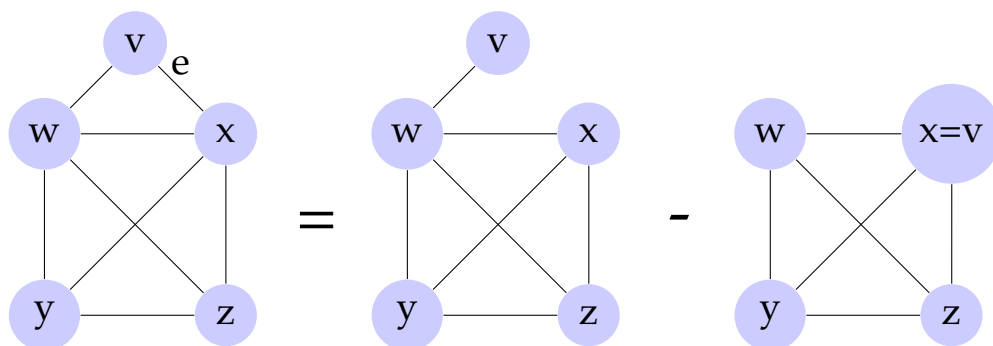
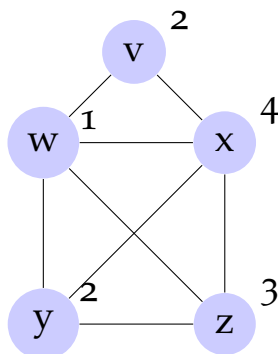
Theorem (Decomposition of Chromatic Polynomials): Let $G = (V, E)$ be a connected graph with $e \in E$. Then

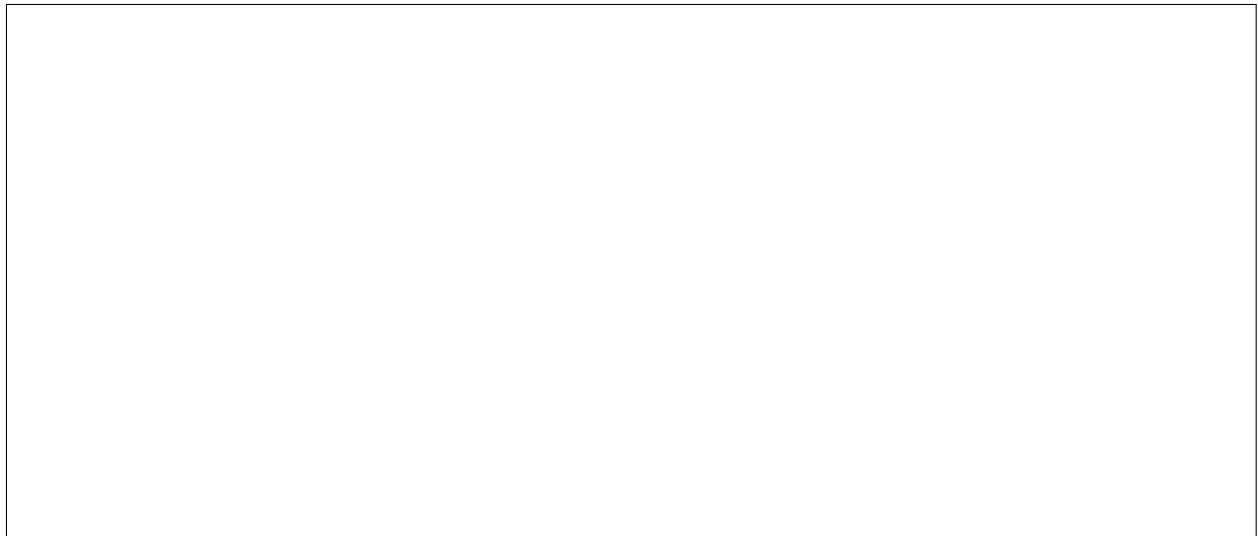
$$P(G_e, \lambda) = P(G, \lambda) + P(G'_e, \lambda).$$

Example 6: Let's use the above theorem to determine $P(G, \lambda)$ for the 4-vertex graph G below.



Example 7: Let's apply the Decomposition Theorem one more time to determine $P(G, \lambda)$ for the 5-vertex graph G below.



**Useful Facts:**

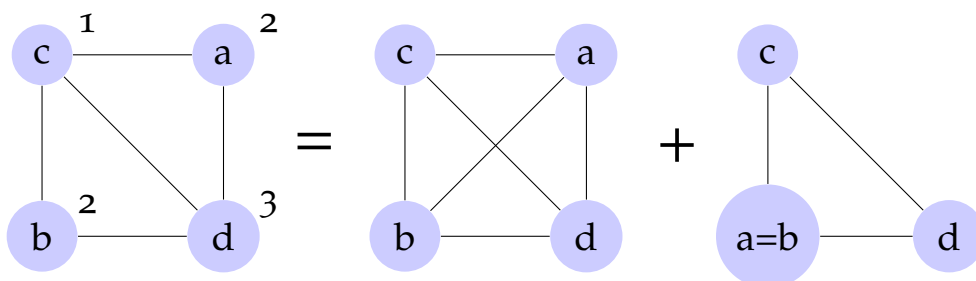
- 1 The constant term in $P(G, \lambda)$ is always zero.
- 2 Provided $|E| > 0$ for $G = (V, E)$, the sum of coefficients in $P(G, \lambda)$ is always zero.

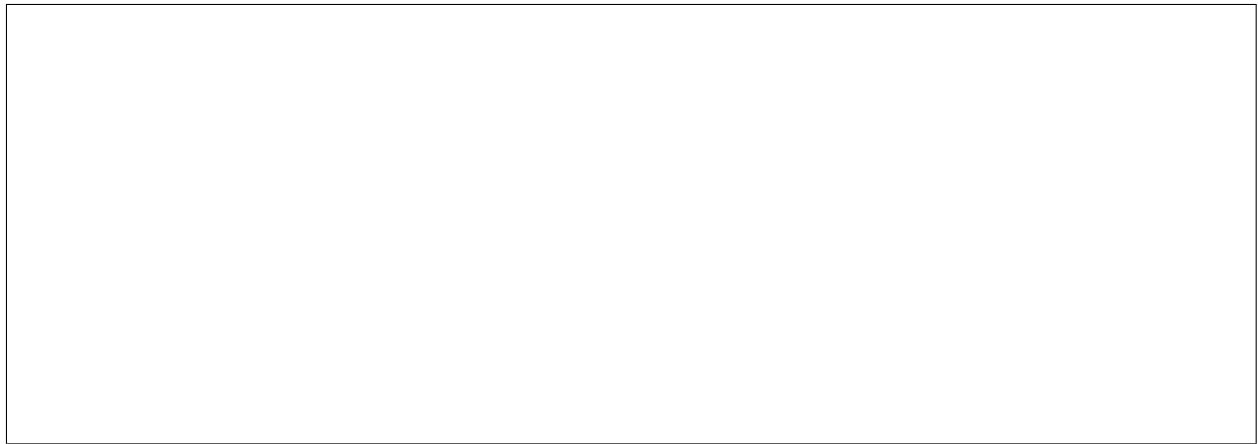
Another approach to get $P(G, \lambda)$ is to add edges toward obtaining a complete graph.

Theorem: Let $G = (V, E)$ with $a, b \in V$ but $\{a, b\} = e \notin E$. Let G_e^+ denote the graph obtained from G by adding the edge $e = \{a, b\}$. Coalescing the vertices a and b in G then yields the subgraph G_e^{++} of G . Then,

$$P(G, \lambda) = P(G_e^+, \lambda) + P(G_e^{++}, \lambda).$$

Example 8: Use the theorem above to determine $P(G, \lambda)$ for the 4-vertex graph G below.





Example 9: Let's revisit the chemical warehouse problem with 7 different chemicals to store. For all $1 \leq i \leq 5$, chemical i cannot be stored in the same compartment as chemical $i + 1$ or $i + 2$.

- a. Determine the smallest number of storage compartments needed to store all seven chemicals.



- b. Suppose these chemical pairs have to be separated: $(1, 4)$, $(2, 5)$, $(2, 6)$, $(3, 6)$. How many compartments would be needed then?

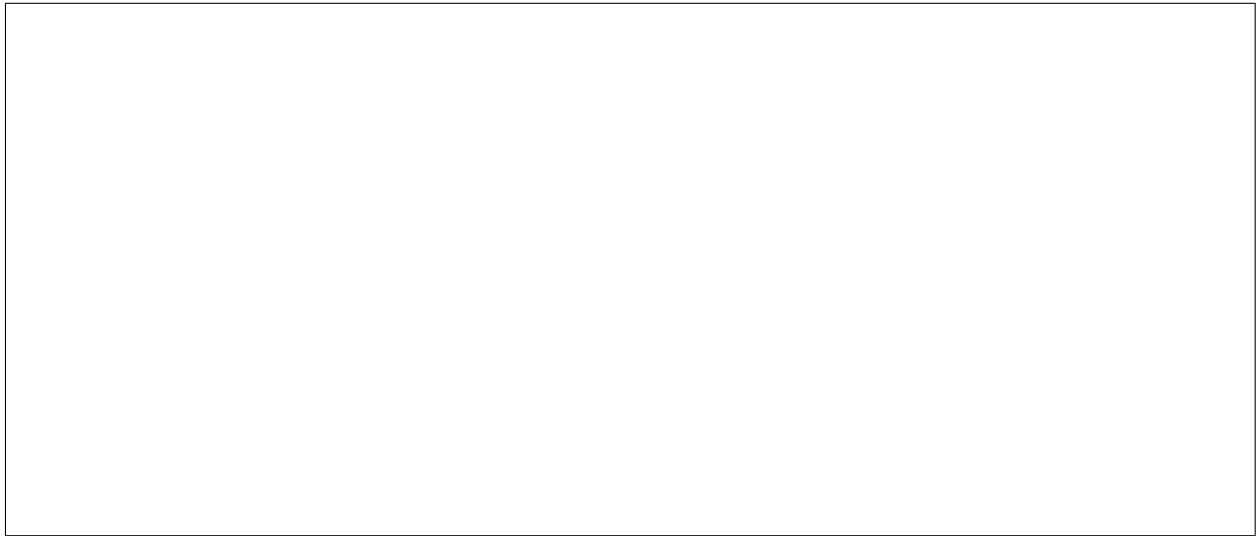


Clustering is a powerful tool in data mining that sorts data into groups or *clusters*. Which athletes are similar, which customers might buy similar products, or what movies are similar are possible applications of data clustering. We will consider data clustering using undirected graphs and a little linear algebra (eigenvectors).

Example: Consider the undirected graph $G = (V, E)$ with $V = \{1, 2, 3, 4, 5, 6, 7\}$ and

$$E = \{ \{1, 6\}, \{1, 4\}, \{4, 6\}, \{2, 4\}, \{2, 5\}, \{2, 7\}, \{5, 7\}, \{3, 5\}, \{3, 7\} \}.$$

Let's draw the connected graph G defined above:



To cluster this graph, we will use an eigenvector of what is defined as the corresponding **Laplacian** matrix to the graph G . To obtain the Laplacian matrix, we first create the adjacency matrix A for the graph in which $a_{ij} = 1$ if there is an edge between vertices i and j ; otherwise, $a_{ij} = 0$. So, for the graph G above, we have

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} .$$

The next step is to create the diagonal matrix D such that d_{ii} is equal to the i th row sum of A . Therefore, we would obtain

$$D = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix} .$$

The Laplacian matrix is defined by $L = D - A$ so that for our graph we would have

$$L = \begin{bmatrix} 2 & 0 & 0 & -1 & 0 & -1 & 0 \\ 0 & 3 & 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 2 & 0 & -1 & 0 & -1 \\ -1 & -1 & 0 & 3 & 0 & -1 & 0 \\ 0 & -1 & -1 & 0 & 3 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 & 2 & 0 \\ 0 & -1 & -1 & 0 & -1 & 0 & 3 \end{bmatrix} .$$

Miroslav Fiedler discovered the importance of the eigenvector say v_2 corresponding to the second smallest eigenvalue of the matrix L for data clustering. Recall from linear algebra (Math 251), an **eigenvector** or characteristic vector of a linear transformation (or matrix) is a non-zero vector that changes by only a scalar factor when that linear transformation is applied to it. In our case, an eigenvector v_i of L and corresponding eigenvalue λ_i satisfy the equation $Lv_i = \lambda_i v_i$. Fiedler proved that the vector v_2 can be used to partition the graph into maximally intraconnected (within cluster) components and minimally interconnected (between clusters) components. The vector v_2 is commonly referred to as the Fiedler vector for the Laplacian matrix L of graph G .

Use of the Fiedler Vector:

Computing the Fiedler vector for the matrix L above we obtain

$$v_2 = \begin{bmatrix} -0.4801 \\ 0.1471 \\ 0.4244 \\ -0.3078 \\ 0.3482 \\ -0.4801 \\ 0.3482 \end{bmatrix} .$$

We can use the vector v_2 to cluster the graph using the signs of each eigenvector component. Vertices of G corresponding to the elements of v_2 that have the same sign are placed into the same cluster. Hence, in our example, nodes/vertices 1, 4, and 6 are placed in one cluster and the remaining nodes/vertices are placed into the other cluster. The min cut for this partitioning (into two graph components) is simply the edge $\{2, 4\}$ of the graph G .

Below is a Python 3 script that will compute the v_2 vector of the graph G . The **numpy** library routine **eig** is used to compute all 7 eigenvalues and corresponding eigenvectors of the Laplacian matrix L .

```
#!/usr/bin/env python3
import numpy as np

# Define the 7 by 7 Laplacian matrix L (by rows) for graph G
A = np.array([[ 2, 0, 0,-1, 0,-1, 0],
              [ 0, 3, 0,-1,-1, 0,-1],
              [ 0, 0, 2, 0,-1, 0,-1],
              [-1,-1, 0, 3, 0,-1, 0],
              [ 0,-1,-1, 0, 3, 0,-1],
              [-1, 0, 0,-1, 0, 2, 0],
              [ 0,-1,-1, 0,-1, 0, 3] ])

# Find the eigenvalues and eigenvectors of L
vals, vecs = np.linalg.eig(A)

# Sort eigenvalues in ascending order (i.e., smallest first)
vecs = vecs[:,np.argsort(vals)]
vals = vals[np.argsort(vals)]

# Print the eigenvector corresponding to the 2nd smallest eigenvalue
# (Python arrays have starting index zero)

for i in range(7) :
    print('\t{:7.4f}'.format(vecs[i,1]))
```

11 PAGERANK ALGORITHM FOR IMPORTANCE RANKING

The PageRank algorithm is commonly used to compute the prestige or importance of vertices (nodes) in the context of Web search. The Web graph consists of pages (nodes) connected by hyperlinks (edges). The algorithm uses the *random surfing* assumption that a user surfing the Web randomly chooses one of the outgoing links from the current page, or with some very small probability randomly jumps to any of the pages in the Web graph. The PageRank of a Web page is defined to be the probability of a random web surfer landing at that page. The PageRank of a node v recursively depends on the PageRank of other nodes that point to it.

11.1 Normalized Importance

Assume that each node u has out-degree of at least 1 and let

$$od(u) = \sum_v A(u, v)$$

denote the out-degree of node u when A is the adjacency matrix for the (directed) Web graph. Hence, $od(u)$ is the sum of the elements in row u in matrix A . Because a random surfer can choose among any of the outgoing links, if there is a link from page u to page v , then the probability of visiting v from u is given by $1/od(u)$.

Starting from an initial probability or PageRank $p_0(u)$ for each node such that

$$\sum_u p_0(u) = 1$$

we can compute an updated PageRank vector for v as follows:

$$p(v) = \sum_u \frac{A(u, v)}{od(u)} \cdot p(u) = \sum_u \frac{N(u, v)}{od(u)} \cdot p(u) = \sum_u \frac{N^T(v, u)}{od(u)} \cdot p(u),$$

where N is the normalized adjacency matrix of the graph defined by

$$N(u, v) = \begin{cases} 1/od(u), & \text{if } (u, v) \in E; \\ 0, & \text{if } (u, v) \notin E. \end{cases}$$

Across all the nodes (pages), we can express the (transposed) PageRank

vector p^T by $p^T = N^T p$.

11.2 Random Jumps

Random surfing is modeled by the assumption of a small probability that a user will jump from one node (page) to any of the other nodes in the graph, even if there are no links between them. You can think of the Web graph as a (virtual) fully-connected directed graph, with an adjacency matrix given by $A_r = \mathbf{1}_{n \times n}$ that has all entries equal to 1. For this random surfer matrix (A_r), the outdegree of each node is $od(u) = n$, and the probability of jumping from node u to any node v is simply $1/od(u) = 1/n$. Thus, if one allows only random jumps from one node to another, the PageRank can be computed as

$$p(v) = \sum_u \frac{N_r^T(v, u)}{od(u)} \cdot p(u),$$

where N_r is the normalized adjacency matrix of the fully-connected Web graph given as $N_r = \frac{1}{n}A_r = \frac{1}{n}\mathbf{1}_{n \times n}$. That is, each element of the $n \times n$ matrix N_r is $1/n$. As discussed in the previous section, the (transposed) PageRank vector p^T across all the nodes for this case would be given by $p^T = N_r^T p$.

11.3 PageRank

The full PageRank is computed by assuming that with some small probability, α , a random Web surfer jumps from the current node u to any other random node v , and with probability $1 - \alpha$ the user follows an existing link from u to v . So, the final (transposed) PageRank vector is defined by

$$p^T = (1 - \alpha)N^T p + \alpha N_r^T p = ((1 - \alpha)N^T + \alpha N_r) p = M^T p,$$

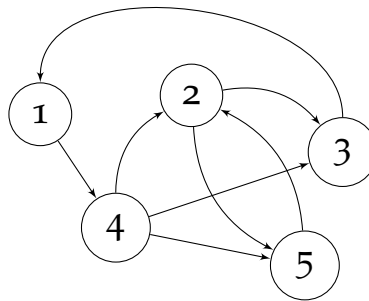
where $M = (1 - \alpha)N + \alpha N_r$ is the combined normalized adjacency matrix. The PageRank vector can be computed iteratively, starting with an initial PageRank assignment p_0 , and updating it in each iteration by $p_{k+1} = M^T p_k$. One minor problem arises if a node u does not have any outgoing edges, i.e., when $odu(u) = 0$. Since there is no outgoing edge from u , the only choice u has is to simply jump to another random node. Thus, we

need to make sure that if $od(u) = 0$, then for the row corresponding to u in M , denoted as M_u , we set $\alpha = 1$, i.e.,

$$M_u = \begin{cases} M_u & \text{if } od(u) > 0, \\ \frac{1}{n} \mathbf{1}_n^T & \text{if } od(u) = 0, \end{cases}$$

where $\mathbf{1}_n$ is the n -dimensional vector of all ones. We can use the power iteration method to compute the dominant eigenvector of M^T .

Example: Consider the directed Web graph¹ $G = (V, E)$ below in which each vertex represents a distinct webpage and each edge (i, j) represents a hyperlink from webpage i to webpage j .



The normalized adjacency matrix N for the Web graph is given by

$$N = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0.5 & 0 & 0.5 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0.33 & 0.33 & 0 & 0.33 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Since there are $n = 5$ nodes (pages) in the Web graph, the normalized

¹*Data Mining and Analysis: Fundamental Concepts and Algorithms*, M.J. Zaki and W. Meira Jr., Cambridge University Press, 2014.

random jump adjacency matrix N_r is given by

$$N_r = \begin{pmatrix} 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \\ 0.2 & 0.2 & 0.2 & 0.2 & 0.2 \end{pmatrix}.$$

Setting $\alpha = 0.1$, the combined normalized adjacency matrix $M = 0.9N + 0.1N_r$ is given by

$$M = \begin{pmatrix} 0.02 & 0.02 & 0.02 & 0.92 & 0.02 \\ 0.02 & 0.02 & 0.47 & 0.02 & 0.47 \\ 0.02 & 0.02 & 0.02 & 0.02 & 0.02 \\ 0.02 & 0.32 & 0.32 & 0.02 & 0.32 \\ 0.02 & 0.92 & 0.02 & 0.02 & 0.02 \end{pmatrix}.$$

Computing the dominant (largest) eigenvalue and corresponding eigenvector of M^T , one can obtain $\lambda = 1$ with $p = (0.419, 0.546, 0.417, 0.422, 0.417)^T$. So for this Web graph, webpage 2 has the highest PageRank value, i.e., the highest probability that a random user would access that webpage.