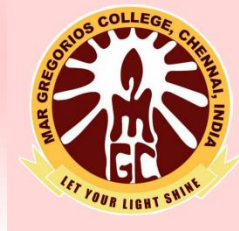


# **MAR GREGORIOS COLLEGE OF ARTS & SCIENCE**

Block No.8, College Road, Mogappair West, Chennai – 37

Affiliated to the University of Madras  
Approved by the Government of Tamil Nadu  
An ISO 9001:2015 Certified Institution



## **DEPARTMENT OF MATHEMATICS**

**SUBJECT NAME: DISCRETE MATHEMATICS**

**SUBJECT CODE: TEM5D**

**SEMESTER: V**

**PREPARED BY: PROF.R.VASUKI**

## SYLLABUS

### UNIT-I

Set , some basic properties of integers , mathematical induction , divisibility of integers , representation of positive integers.

### UNIT – II

Boolean algebra , two element Boolean algebra , disjunctive normal form , conjunctive normal form .

### UNIT – III

Application , Simplification of circuits , designing of switching circuits , logical gates and combinatorial circuits .

### UNIT- IV

Sequence and recurrence relation , solving recurrence relation by iteration method , modeling of counting problems by recurrence relations , linear ( difference equations ) recurrence relations with constant coefficients , generating functions , sum and product of two generating functions , useful generating functions , combinatorial problems .

### UNIT – V

Introduction , walk , path and cycles , Euler circuits

# UNIT 1

## Basic Set Theory

**A set is a Many that allows itself to be thought of as a One.**

- Georg Cantor

This chapter introduces set theory, mathematical induction, and formalizes the notion of mathematical functions. The material is mostly elementary. For those of you new to abstract mathematics elementary does not mean *simple* (though much of the material is fairly simple). Rather, elementary means that the material requires very little previous education to understand it. Elementary material can be quite challenging and some of the material in this chapter, if not exactly rocket science, may require that you adjust your point of view to understand it. The single most powerful technique in mathematics is to adjust your point of view until the problem you are trying to solve becomes simple.

Another point at which this material may diverge from your previous experience is that it will require proof. In standard introductory classes in algebra, trigonometry, and calculus there is currently very little emphasis on the discipline of *proof*. Proof is, however, the central tool of mathematics. This text is for a course that is a student's formal introduction to tools and methods of proof.

### 2.1 Set Theory

A *set* is a collection of distinct objects. This means that  $\{1, 2, 3\}$  is a set but  $\{1, 1, 3\}$  is not because 1 appears twice in the second collection. The second collection is called a *multiset*. Sets are often specified with curly brace notation. The set of even integers

can be written:

$$\{2n : n \text{ is an integer}\}$$

The opening and closing curly braces denote a set,  $2n$  specifies the members of the set, the colon says “such that” or “where” and everything following the colon are conditions that explain or refine the membership. All correct mathematics can be spoken in English. The set definition above is spoken “The set of twice  $n$  where  $n$  is an integer”.

The only problem with this definition is that we do not yet have a formal definition of the integers. The integers are the set of whole numbers, both positive and negative:  $\{0, \pm 1, \pm 2, \pm 3, \dots\}$ . We now introduce the operations used to manipulate sets, using the opportunity to practice curly brace notation.

**Definition 1** *The empty set is a set containing no objects. It is written as a pair of curly braces with nothing inside  $\{\}$  or by using the symbol  $\emptyset$ .*

As we shall see, the empty set is a handy object. It is also quite strange. The set of all humans that weigh at least eight tons, for example, is the empty set. Sets whose definition contains a contradiction or impossibility are often empty.

**Definition 2** *The set membership symbol  $\in$  is used to say that an object is a member of a set. It has a partner symbol  $\notin$  which is used to say an object is not in a set.*

**Definition 3** *We say two sets are equal if they have exactly the same members.*

**Example** If

$$S = \{1, 2, 3\}$$

then  $3 \in S$  and  $4 \notin S$ . The set membership symbol is often used in defining operations that manipulate sets. The set

$$T = \{2, 3, 1\}$$

is equal to  $S$  because they have the same members: 1, 2, and 3. While we usually list the members of a set in a “standard” order (if one is available) there is no requirement to do so and sets are indifferent to the order in which their members are listed.

**Definition 4** The **cardinality** of a set is its size. For a finite set, the cardinality of a set is the number of members it contains. In symbolic notation the size of a set  $S$  is written  $|S|$ . We will deal with the idea of the cardinality of an infinite set later.

**Example 2 Set cardinality**

For the set  $S = \{1, 2, 3\}$  we show cardinality by writing  $|S| = 3$

We now move on to a number of *operations* on sets. You are already familiar with several operations on numbers such as addition, multiplication, and negation.

**Definition 2** The **intersection** of two sets  $S$  and  $T$  is the collection of all objects that are in both sets. It is written  $S \cap T$ . Using curly brace notation

$$S \cap T = \{x : (x \in S) \text{ and } (x \in T)\}$$

The symbol *and* in the above definition is an example of a Boolean or logical operation. It is only true when both the propositions it joins are also true. It has a symbolic equivalent  $\wedge$ . This lets us write the formal definition of intersection more compactly:

$$S \cap T = \{x : (x \in S) \wedge (x \in T)\}$$

**Example 3 Intersections of sets**

Suppose  $S = \{1, 2, 3, 5\}$ ,  
 $T = \{1, 3, 4, 5\}$ , and  $U = \{2, 3, 4, 5\}$ .  
Then:

$$S \cap T = \{1, 3, 5\},$$

$$S \cap U = \{2, 3, 5\}, \text{ and}$$

$$T \cap U = \{3, 4, 5\}$$

**Definition 6** If  $A$  and  $B$  are sets and  $A \cap B = \emptyset$  then we say that  $A$  and  $B$  are disjoint, or disjoint sets.

**Definition 7** The **union** of two sets  $S$  and  $T$  is the collection of all objects that are in either set. It is written  $S \cup T$ . Using curly brace notation

$$S \cup T = \{x : (x \in S) \text{ or } (x \in T)\}$$

The symbol *or* is another Boolean operation, one that is true if either of the propositions it joins are true. Its symbolic equivalent is  $\vee$  which lets us re-write the definition of union as:

$$S \cup T = \{x : (x \in S) \vee (x \in T)\}$$

**Example 2 Unions of sets.**

Suppose  $S = \{1, 2, 3\}$ ,  $T = \{1, 3, 5\}$ , and  $U = \{2, 3, 4, 5\}$ .

Then:

$$S \cup T = \{1, 2, 3, 5\},$$

$$S \cup U = \{1, 2, 3, 4, 5\}, \text{ and}$$

$$T \cup U = \{1, 2, 3, 4, 5\}$$

When performing set theoretic computations, you should declare the domain in which you are working. In set theory this is done by declaring a universal set.

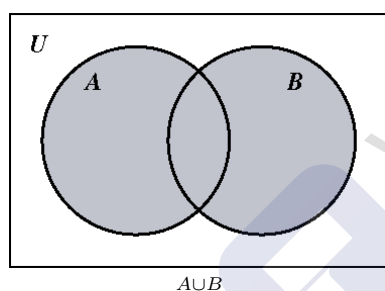
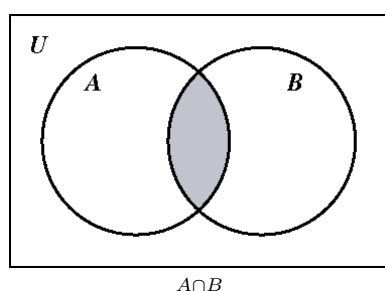
**Definition 8** The **universal set**, at least for a given collection of set theoretic computations, is the set of all possible objects.

If we declare our universal set to be the integers then  $\{\frac{1}{2}, \frac{2}{3}\}$  is not a well defined set because the objects used to define it are not members of the universal set. The symbols  $\{\frac{1}{2}, \frac{2}{3}\}$  do define a set if a universal set that includes  $\frac{1}{2}$  and  $\frac{2}{3}$  is chosen. The problem arises from the fact that neither of these numbers are integers. The universal set is commonly written  $\mathcal{U}$ . Now that we have the idea of declaring a universal set we can define another operation on sets.

## Venn Diagrams

A Venn diagram is a way of depicting the relationship between sets. Each set is shown as a circle and circles overlap if the sets intersect.

**Example 5** The following are Venn diagrams for the intersection and union of two sets. The shaded parts of the diagrams are the intersections and unions respectively.



Notice that the rectangle containing the diagram is labeled with a  $U$  representing the universal set.

**Definition 9** The **compliment** of a set  $S$  is the collection of objects in the universal set that are not in  $S$ . The compliment is written  $S^c$ . In curly brace notation

$$S^c = \{x : (x \in U) \wedge (x \notin S)\}$$

or more compactly as

$$S^c = \{x : x \notin S\}$$

however it should be apparent that the compliment of a set always depends on which universal set is chosen.

There is also a Boolean symbol associated with the complementation operation: the *not* operation. The

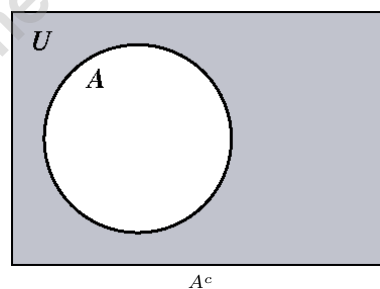
notation for not is  $\neg$ . There is not much savings in space as the definition of compliment becomes

$$S^c = \{x : \neg(x \in S)\}$$

## Example 6 Set Compliments

- (i) Let the universal set be the integers. Then the compliment of the even integers is the odd integers.
- (ii) Let the universal set be  $\{1, 2, 3, 4, 5\}$ , then the compliment of  $S = \{1, 2, 3\}$  is  $S^c = \{4, 5\}$  while the compliment of  $T = \{1, 3, 5\}$  is  $T^c = \{2, 4\}$ .
- (iii) Let the universal set be the letters  $\{a, e, i, o, u, y\}$ . Then  $\{y\}^c = \{a, e, i, o, u\}$ .

The Venn diagram for  $A^c$  is



We now have enough set-theory operators to use them to define more operators quickly. We will continue to give English and symbolic definitions.

**Definition 10** The **difference** of two sets  $S$  and  $T$  is the collection of objects in  $S$  that are not in  $T$ . The difference is written  $S - T$ . In curly brace notation

$$S - T = \{x : x \in (S \cap (T^c))\},$$

or alternately

$$S - T = \{x : (x \in S) \wedge (x \notin T)\}$$

Notice how intersection and complementation can be used together to create the difference operation and that the definition can be rephrased to use Boolean operations. There is a set of rules that reduces the number of parenthesis required. These are called **operator precedence rules**.

- (i) Other things being equal, operations are performed left-to-right.
- (ii) Operations between parenthesis are done first, starting with the innermost of nested parenthesis.
- (iii) All complementations are computed next.
- (iv) All intersections are done next.
- (v) All unions are performed next.
- (vi) Tests of set membership and computations, equality or inequality are performed last.

Special operations like the set difference or the symmetric difference, defined below, are not included in the precedence rules and thus always use parenthesis.

#### Example 7 Operator precedence

Since complementation is done before intersection the symbolic definition of the difference of sets can be rewritten:

$$S - T = \{x : x \in S \cap T^c\}$$

If we were to take the set operations

$$A \cup B \cap C^c$$

and put in the parenthesis we would get

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

**Definition 11** The **symmetric difference** of two sets  $S$  and  $T$  is the set of objects that are in one and only one of the sets. The symmetric difference is written  $S\Delta T$ . In curly brace notation:

$$S\Delta T = \{(S - T) \cup (T - S)\}$$

#### Example 8 Symmetric differences

Let  $S$  be the set of non-negative multiples of two that are no more than twenty four. Let  $T$  be the non-negative multiples of three that are no more than twenty four. Then

$$S\Delta T = \{2, 3, 4, 8, 9, 10, 14, 15, 16, 20, 21, 22\}$$

Another way to think about this is that we need numbers that are positive multiples of 2 or 3 (but not both) that are no more than 24.

Another important tool for working with sets is the ability to compare them. We have already defined what it means for two sets to be equal, and so by implication what it means for them to be unequal. We now define another comparator for sets.

**Definition 12** For two sets  $S$  and  $T$  we say that  $S$  is a **subset** of  $T$  if each element of  $S$  is also an element of  $T$ . In formal notation  $S \subseteq T$  if for all  $x \in S$  we have  $x \in T$ .

If  $S \subseteq T$  then we also say  $T$  contains  $S$  which can be written  $T \supseteq S$ . If  $S \subseteq T$  and  $S \neq T$  then we write  $S \subset T$  and we say  $S$  is a *proper* subset of  $T$ .

#### Example 9 Subsets

If  $A = \{a, b, c\}$  then  $A$  has eight different subsets:

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

Notice that  $A \subseteq A$  and in fact each set is a subset of itself. The empty set  $\emptyset$  is a subset of every set.

We are now ready to prove our first proposition. Some new notation is required and we must introduce an important piece of mathematical culture. If we say “A if and only if B” then we mean that either A and B are both true or they are both false in any given circumstance. For example: “an integer  $x$  is even if and only if it is a multiple of 2”. The phrase “if and only if” is used to establish *logical equivalence*. Mathematically, “A if and only if B” is a way of stating that A and B are simply different ways of saying the same thing. The phrase “if and only if” is abbreviated iff and is represented symbolically as the double arrow  $\Leftrightarrow$ . Proving an iff statement is done by independently demonstrating that each may be deduced from the other.

**Proposition 1** Two sets are equal if and only if each is a subset of the other. In symbolic notation:

$$(A = B) \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

Proof:

Let the two sets in question be  $A$  and  $B$ . Begin by assuming that  $A = B$ . We know that every set is

a subset of itself so  $A \subseteq A$ . Since  $A = B$  we may substitute into this expression on the left and obtain  $B \subseteq A$ . Similarly we may substitute on the right and obtain  $A \subseteq B$ . We have thus demonstrated that if  $A = B$  then  $A$  and  $B$  are both subsets of each other, giving us the first half of the iff.

Assume now that  $A \subseteq B$  and  $B \subseteq A$ . Then the definition of subset tells us that any element of  $A$  is an element of  $B$ . Similarly any element of  $B$  is an element of  $A$ . This means that  $A$  and  $B$  have the same elements which satisfies the definition of set equality. We deduce  $A = B$  and we have the second half of the iff.  $\square$

A note on mathematical grammar: the symbol  $\square$  indicates the end of a proof. On a paper turned in by a student it is usually taken to mean “I think the proof ends here”. Any proof should have a  $\square$  to indicate its end. The student should also note the lack of calculations in the above proof. If a proof cannot be read back in (sometimes overly formal) English then it is probably incorrect. Mathematical symbols should be used for the sake of brevity or clarity, not to obscure meaning.

**Proposition 2 De Morgan’s Laws** *Suppose that  $S$  and  $T$  are sets. DeMorgan’s Laws state that*

$$(i) (S \cup T)^c = S^c \cap T^c, \text{ and}$$

$$(ii) (S \cap T)^c = S^c \cup T^c.$$

Proof:

Let  $x \in (S \cup T)^c$ ; then  $x$  is not a member of  $S$  or  $T$ . Since  $x$  is not a member of  $S$  we see that  $x \in S^c$ . Similarly  $x \in T^c$ . Since  $x$  is a member of both these sets we see that  $x \in S^c \cap T^c$  and we see that  $(S \cup T)^c \subseteq S^c \cap T^c$ . Let  $y \in S^c \cap T^c$ . Then the definition of intersection tells us that  $y \in S^c$  and  $y \in T^c$ . This in turn lets us deduce that  $y$  is not a member of  $S \cup T$ , since it is not in either set, and so we see that  $y \in (S \cup T)^c$ . This demonstrates that  $S^c \cap T^c \subseteq (S \cup T)^c$ . Applying Proposition 2.1 we get that  $(S \cup T)^c = S^c \cap T^c$  and we have proven part (i). The proof of part (ii) is left as an exercise.  $\square$

In order to prove a mathematical statement you must prove it is always true. In order to disprove a mathematical statement you need only find a single instance

where it is false. It is thus possible for a false mathematical statement to be “true most of the time”. In the next chapter we will develop the theory of prime numbers. For now we will assume the reader has a modest familiarity with the primes. The statement “Prime numbers are odd” is false once, because 2 is a prime number. All the other prime numbers are odd. The statement is a false one. This very strict definition of what makes a statement true is a convention in mathematics. We call 2 a *counter example*. It is thus necessary to find only one counter-example to demonstrate a statement is (mathematically) false.

### Example 10 Disproof by counter example

*Prove that the statement  $A \cup B = A \cap B$  is false.*

*Let  $A = \{1, 2\}$  and  $B = \{3, 4\}$ . Then  $A \cap B = \emptyset$  while  $A \cup B = \{1, 2, 3, 4\}$ . The sets  $A$  and  $B$  form a counter-example to the statement.*

## Problems

**Problem 1** *Which of the following are sets? Assume that a proper universal set has been chosen and answer by listing the names of the collections of objects that are sets. Warning: at least one of these items has an answer that, while likely, is not 100% certain.*

$$(i) A = \{2, 3, 5, 7, 11, 13, 19\}$$

$$(ii) B = \{A, E, I, O, U\}$$

$$(iii) C = \{\sqrt{x} : x < 0\}$$

$$(iv) D = \{1, 2, A, 5, B, Q, 1, V\}$$

(v)  $E$  is the list of first names of people in the 1972 phone book in Lawrence Kansas in the order they appear in the book. There were more than 35,000 people in Lawrence that year.

(vi)  $F$  is a list of the weight, to the nearest kilogram, of all people that were in Canada at any time in 2007.

(vii)  $G$  is a list of all weights, to the nearest kilogram, that at least one person in Canada had in 2007.

**Problem 2** Suppose that we have the set  $U = \{n : 0 \leq n < 100\}$  of whole numbers as our universal set. Let  $P$  be the prime numbers in  $U$ , let  $E$  be the even numbers in  $U$ , and let  $F = \{1, 2, 3, 5, 8, 13, 21, 34, 55, 89\}$ . Describe the following sets either by listing them or with a careful English sentence.

- (i)  $E^c$ ,
- (ii)  $P \cap F$ ,
- (iii)  $P \cap E$ ,
- (iv)  $F \cap E \cup F \cap E^c$ , and
- (v)  $F \cup F^c$ .

**Problem 3** Suppose that we take the universal set  $U$  to be the integers. Let  $S$  be the even integers, let  $T$  be the integers that can be obtained by tripling any one integer and adding one to it, and let  $V$  be the set of numbers that are whole multiples of both two and three.

- (i) Write  $S$ ,  $T$ , and  $V$  using symbolic notation.
- (ii) Compute  $S \cap T$ ,  $S \cap V$  and  $T \cap V$  and give symbolic representations that do not use the symbols  $S$ ,  $T$ , or  $V$  on the right hand side of the equals sign.

**Problem 4** Compute the cardinality of the following sets. You may use other texts or the internet.

- (i) Two digit positive odd integers.
- (ii) Elements present in a sucrose molecule.
- (iii) Isotopes of hydrogen that are not radioactive.
- (iv) Planets orbiting the same star as the planet you are standing on that have moons. Assume that Pluto is a minor planet.
- (v) Elements with seven electrons in their valence shell. Remember that Ununoctium was discovered in 2002 so be sure to use a relatively recent reference.
- (vi) Subsets of  $S = \{a, b, c, d\}$  with cardinality 2.
- (vii) Prime numbers whose base-ten digits sum to ten. Be careful, some have three digits.

**Problem 5** Find an example of an infinite set that has a finite complement, be sure to state the universal set.

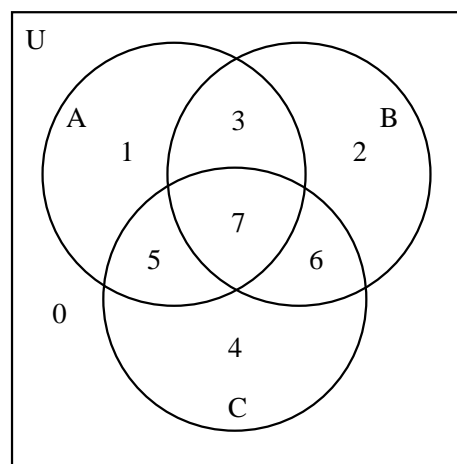
**Problem 6** Find an example of an infinite set that has an infinite complement, be sure to state the universal set.

**Problem 7** Add parenthesis to each of the following expressions that enforce the operator precedence rules as in Example 2.7. Notice that the first three describe sets while the last returns a logical value (true or false).

- (i)  $A \cup B \cup C \cup D$
- (ii)  $A \cup B \cap C \cup D$
- (iii)  $A^c \cap B^c \cup C$
- (iv)  $A \cup B = A \cap C$

**Problem 8** Give the Venn diagrams for the following sets.

- (i)  $A - B$  (ii)  $B - A$  (iii)  $A^c \cap B$
- (iv)  $A \Delta B$  (v)  $(A \Delta B)^c$  (vi)  $A^c \cup B^c$



**Problem 9** Examine the Venn diagram above. Notice that every combination of sets has a unique number in common. Construct a similar collection of four sets.

**Problem 10** Read Problem 2.9. Can a system of sets of this sort be constructed for any number of sets? Explain your reasoning.



## MATHEMATICAL INDUCTION

**Problem 11** Suppose we take the universal set to be the set of non-negative integers. Let  $E$  be the set of even numbers,  $O$  be the set of odd numbers and  $F = \{0, 1, 2, 3, 5, 8, 13, 21, 34, 89, 144, \dots\}$  be the set of Fibonacci numbers. The Fibonacci sequence is  $0, 1, 1, 2, 3, 5, 8, \dots$  in which the next term is obtained by adding the previous two.

- (i) Prove that the intersection of  $F$  with  $E$  and  $O$  are both infinite.
- (ii) Make a Venn diagram for the sets  $E$ ,  $F$ , and  $O$ , and explain why this is a Mickey-Mouse problem.

**Problem 12** A binary operation  $\odot$  is commutative if  $x \odot y = y \odot x$ . An example of a commutative operation is multiplication. Subtraction is non-commutative. Determine, with proof, if union, intersection, set difference, and symmetric difference are commutative.

**Problem 13** An identity for an operation  $\odot$  is an object  $i$  so that, for all objects  $x$ ,  $i \odot x = x \odot i = x$ . Find, with proof, identities for the operations set union and set intersection.

**Problem 14** Prove part (ii) of Proposition 2.2.

**Problem 15** Prove that

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

**Problem 16** Prove that

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

**Problem 17** Prove that

$$A \Delta (B \Delta C) = (A \Delta B) \Delta C$$

**Problem 18** Disprove that

$$A \Delta (B \cup C) = (A \Delta B) \cup C$$

**Problem 19** Consider the set  $S = \{1, 2, 3, 4\}$ . For each  $k = 0, 1, \dots, 4$  how many  $k$  element subsets does  $S$  have?

**Problem 20** Suppose we have a set  $S$  with  $n \geq 0$  elements. Find a formula for the number of different subsets of  $S$  that have  $k$  elements.

**Problem 21** For finite sets  $S$  and  $T$ , prove

$$|S \cup T| = |S| + |T| - |S \cap T|$$

## Mathematical Induction

Mathematical induction is a technique used in proving mathematical assertions. The basic idea of induction is that we prove that a statement is true in one case and then also prove that if it is true in a given case it is true in the next case. This then permits the cases for which the statement is true to cascade from the initial true case. We will start with the mathematical foundations of induction.

We assume that the reader is familiar with the symbols  $<$ ,  $>$ ,  $\leq$  and  $\geq$ . From this point on we will denote the set of integers by the symbol  $\mathbb{Z}$ . The non-negative integers are called the *natural numbers*. The symbol for the set of natural numbers is  $\mathbb{N}$ . Any mathematical system rests on a foundation of axioms. Axioms are things that we simply assume to be true. We will assume the truth of the following principle, adopting it as an axiom.

**The well-ordering principle:** Every non-empty set of natural numbers contains a smallest element.

The well ordering principle is an axiom that agrees with the common sense of most people familiar with the natural numbers. An empty set does not contain a smallest member because it contains no members at all. As soon as we have a set of natural numbers with some members then we can order those members in the usual fashion. Having ordered them, one will be smallest. This intuition agreeing with this latter claim depends strongly on the fact the integers are “whole numbers” spaced out in increments of one. To see why this is important consider the smallest positive distance. If such a distance existed, we could cut it in half to obtain a smaller distance - the quantity contradicts its own existence. The well-ordering principle can be used to prove the correctness of induction.

**Theorem - Mathematical Induction I** Suppose that  $P(n)$  is a proposition that is either true or false for any given natural number  $n$ . If

(i)  $P(0)$  is true and,

(ii) when  $P(n)$  is true so is  $P(n+1)$

Then we may deduce that  $P(n)$  is true for any natural number.

Proof

:

Assume that (i) and (ii) are both true statements. Let  $S$  be the set of all natural numbers for which  $P(n)$  is false. If  $S$  is empty then we are done, so assume that  $S$  is not empty. Then, by the well ordering principle,  $S$  has a least member  $m$ . By (i) above  $m \neq 0$  and so  $m - 1$  is a natural number. Since  $m$  is the smallest member of  $S$  it follows that  $P(m-1)$  is true. But this means, by (ii) above, that  $P(m)$  is true. We have a contradiction and so our assumption that  $S \neq \emptyset$  must be wrong. We deduce  $S$  is empty and that as a consequence  $P(n)$  is true for all  $n \in \mathbb{N}$ .  $\square$

The technique used in the above proof is called *proof by contradiction*. We start by assuming the logical opposite of what we want to prove, in this case that there is some  $m$  for which  $P(m)$  is false, and from that assumption we derive an impossibility. If an assumption can be used to demonstrate an impossibility then it is false and its logical opposite is true.

A nice problem on which to demonstrate mathematical induction is counting how many subsets a finite set has.

**Proposition 3 Subset counting.** *A set  $S$  with  $n$  elements has  $2^n$  subsets.*

Proof:

First we check that the proposition is true when  $n = 0$ . The empty set has exactly one subset: itself. Since  $2^0 = 1$  the proposition is true for  $n = 0$ . We now assume the proposition is true for some  $n$ . Suppose that  $S$  is a set with  $n + 1$  members and that  $x \in S$ . Then  $S - \{x\}$  (the set difference of  $S$  and a set  $\{x\}$  containing only  $x$ ) is a set of  $n$  elements and so, by the assumption, has  $2^n$  subsets. Now every subset of  $S$  either contains  $x$  or it fails to. Every subset of  $S$  that does not contain  $x$  is a subset of  $S - \{x\}$  and so there are  $2^n$  such subsets of  $S$ . Every subset of  $S$  that contains  $x$  may be obtained in exactly one way from one that does not by taking the union with  $\{x\}$ . This means that the number of subsets of  $S$  containing or failing to contain  $x$  are equal. This means there are  $2^n$  subsets of  $S$  containing  $x$ . The total number of subsets of  $S$  is thus  $2^n + 2^n = 2^{n+1}$ . So if we assume the proposition is true for  $n$  we can demonstrate that it is also true for  $n + 1$ . It follows by mathematical

induction that the proposition is true for all natural numbers.  $\square$

The set of all subsets of a given set is itself an important object and so has a name.

**Definition 13** *The set of all subsets of a set  $S$  is called the powerset of  $S$ . The notation for the powerset of  $S$  is  $\mathcal{P}(S)$ .*

This definition permits us to rephrase Proposition 2.3 as follows: the power set of a set of  $n$  elements has size  $2^n$ .

Theorem 2.1 lets us prove propositions that are true on the natural numbers, starting at zero. A small modification of induction can be used to prove statements that are true only for those  $n \geq k$  for any integer  $k$ . All that is needed is to use induction on a proposition  $Q(n - k)$  where  $Q(n - k)$  is logically equivalent to  $P(n)$ . If  $Q(n - k)$  is true for  $n - k \geq 0$  then  $P(n)$  is true for  $n \geq k$  and we have the modified induction. The practical difference is that we start with  $k$  instead of zero.

**Example 11** *Prove that  $n^2 \geq 2n$  for all  $n \geq 2$ .*

Notice that  $2^2 = 4 = 2 \times 2$  so the proposition is true when  $n = 2$ . We next assume that  $P(n)$  is true for some  $n$  and we compute:

$$\begin{aligned} n^2 &\geq 2n \\ n^2 + 2n + 1 &\geq 2n + 2n + 1 \\ (n + 1)^2 &\geq 2n + 2n + 1 \\ (n + 1)^2 &\geq 2n + 1 + 1 \\ (n + 1)^2 &\geq 2n + 2 \\ (n + 1)^2 &\geq 2(n + 1) \end{aligned}$$

To move from the third step to the fourth step we use the fact that  $2n > 1$  when  $n \geq 2$ . The last step is  $P(n + 1)$ , which means we have deduced  $P(n + 1)$  from  $P(n)$ . Using the modified form of induction we have proved that  $n^2 \geq 2n$  for all  $n \geq 2$ .

It is possible to formalize the procedure for using mathematical induction into a three-part process. Once we have a proposition  $P(n)$ ,

### MATHEMATICAL INDUCTION

- (i) First demonstrate a *base case* by directly demonstrating  $P(k)$ ,
- (ii) Next make the *induction hypothesis* that  $P(n)$  is true for some  $n$ ,
- (iii) Finally, starting with the assumption that  $P(n)$  is true, demonstrate  $P(n + 1)$ .

These steps permit us to deduce that  $P(n)$  is true for all  $n \geq k$ .

**Example 12** Using induction, prove

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

In this case  $P(n)$  is the statement

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

**Base case:**  $1 = \frac{1}{2}1(1 + 1)$ , so  $P(1)$  is true. **Induction hypothesis:** for some  $n$ ,

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

Compute:

$$\begin{aligned} 1 + 2 + \cdots + (n + 1) &= 1 + 2 + \cdots + n + (n + 1) \\ &= \frac{1}{2}n(n + 1) + (n + 1) \\ &= \frac{1}{2}(n(n + 1) + 2(n + 1)) \\ &= \frac{1}{2}(n^2 + 3n + 2) \\ &= \frac{1}{2}(n + 1)(n + 2) \\ &= \frac{1}{2}(n + 1)((n + 1) + 1) \end{aligned}$$

and so we have shown that if  $P(n)$  is true then so is  $P(n + 1)$ . We have thus proven that  $P(n)$  is true for all  $n \geq 1$  by mathematical induction.

We now introduce *sigma notation* which makes problems like the one worked in Example 2.12 easier to state and manipulate. The symbol  $\sum$  is used to add

up lists of numbers. If we wished to sum some formula  $f(i)$  over a range from  $a$  to  $b$ , that is to say  $a \leq i \leq b$ , then we write :

$$\sum_{i=a}^b f(i)$$

On the other hand if  $S$  is a set of numbers and we want to add up  $f(s)$  for all  $s \in S$  we write:

$$\sum_{s \in S} f(s)$$

The result proved in Example 2.12 may be stated in the following form using sigma notation.

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

**Proposition 4** Suppose that  $c$  is a constant and that  $f(i)$  and  $g(i)$  are formulas. Then

$$(i) \sum_{i=a}^b (f(i) + g(i)) = \sum_{i=a}^b f(i) + \sum_{i=a}^b g(i)$$

$$(ii) \sum_{i=a}^b (f(i) - g(i)) = \sum_{i=a}^b f(i) - \sum_{i=a}^b g(i)$$

$$(iii) \sum_{i=a}^b c \cdot f(i) = c \cdot \sum_{i=a}^b f(i).$$

Proof:

Part (i) and (ii) are both simply the associative law for addition:  $a + (b + c) = (a + b) + c$  applied many times. Part (iii) is a similar multiple application of the distributive law  $ca + cb = c(a + b)$ .  $\square$

The sigma notation lets us work with indefinitely long (and even infinite) sums. There are other similar notations. If  $A_1, A_2, \dots, A_n$  are sets then the intersection or union of all these sets can be written:

$$\bigcap_{i=1}^n A_i$$

$$\bigcup_{i=1}^n A_i$$

Similarly if  $f(i)$  is a formula on the integers then

$$\prod_{i=1}^n f(i)$$

is the notation for computing the product  $f(1) \cdot f(2) \cdot \cdots \cdot f(n)$ . This notation is called **Pi** notation.

**Definition 14** When we solve an expression involving  $\sum$  to obtain a formula that does not use  $\sum$  or  $\dots$  as in Example 2.12 then we say we have found a closed form for the expression. Example 2.12 finds a closed form for  $\sum_{i=1}^n i$ .

At this point we introduce a famous mathematical sequence in order to create an arena for practicing proofs by induction.

**Definition 15** The **Fibonacci numbers** are defined as follows.  $f_1 = f_2 = 1$  and, for  $n \geq 3$ ,  $f_n = f_{n-1} + f_{n-2}$ .

**Example 13** The Fibonacci numbers with four or fewer digits are:  $f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, f_8 = 21, f_9 = 34, f_{10} = 55, f_{11} = 89, f_{12} = 144, f_{13} = 233, f_{14} = 377, f_{15} = 610, f_{16} = 987, f_{17} = 1597, f_{18} = 2584, f_{19} = 4181, \text{ and } f_{20} = 6765$ .

**Example 14** Prove that the Fibonacci number  $f_{3n}$  is even.

**Solution:**

Notice that  $f_3 = 2$  and so the proposition is true when  $n = 1$ . Assume that the proposition is true for some  $n \geq 1$ . Then:

$$f_{3(n+1)} = f_{3n+3} \quad (2.1)$$

$$= f_{3n+2} + f_{3n+1} \quad (2.2)$$

$$= f_{3n+1} + f_{3n} + f_{3n+1} \quad (2.3)$$

$$= 2 \cdot f_{3n+1} + f_{3n} \quad (2.4)$$

but this suffices because  $f_{3n}$  is even by the induction hypothesis while  $2 \cdot f_{3n+1}$  is also even. The sum is thus even and so  $f_{3(n+1)}$  is even. It follows by induction that  $f_{3n}$  is even for all  $n$ .  $\square$

## Problems

**Problem 22** Suppose that  $S = \{a, b, c\}$ . Compute and list explicitly the members of the powerset,  $\mathcal{P}(S)$ .

**Problem 23** Prove that for a finite set  $X$  that

$$|X| \leq |\mathcal{P}(X)|$$

**Problem 24** Suppose that  $X \subseteq Y$  with  $|Y| = n$  and  $|X| = m$ . Compute the number of subsets of  $Y$  that contain  $X$ .

**Problem 25** Compute the following sums.

(i)  $\sum_{i=1}^{20} i$ ,

(ii)  $\sum_{i=10}^{30} i$ , and

(iii)  $\sum_{i=-20}^{21} i$ .

**Problem 26** Using mathematical induction, prove the following formulas.

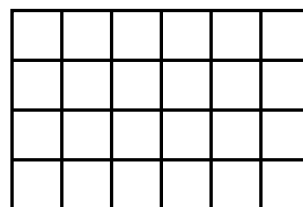
(i)  $\sum_{i=1}^n 1 = n$ ,

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

(iii)  $\sum_{i=1}^n i^3 = \frac{n^2(n+1)^2}{4}$ .

**Problem 27** If  $f(i)$  and  $g(i)$  are formulas and  $c$  and  $d$  are constants prove that

$$\sum_{i=a}^b (c \cdot f(i) + d \cdot g(i)) = c \cdot \sum_{i=a}^b f(i) + d \cdot \sum_{i=a}^b g(i)$$



**Problem 28** Suppose you want to break an  $n \times m$  chocolate bar, like the  $6 \times 4$  example shown above, into pieces corresponding to the small squares shown. What is the minimum number of breaks you can make? Prove your answer is correct.

**Problem 29** Prove by induction that the sum of the first  $n$  odd numbers equals  $n^2$ .

**Problem 30** Compute the sum of the first  $n$  positive even numbers.

**Problem 31** Find a closed form for

$$\sum_{i=1}^n i^2 + 3i + 5$$

**Problem 32** Let  $f(n, 3)$  be the number of subsets of  $\{1, 2, \dots, n\}$  of size 3. Using induction, prove that  $f(n, 3) = \frac{1}{6}n(n-1)(n-2)$ .

**Problem 33** Suppose that we have sets  $X_1, X_2, \dots, X_n$  and  $Y_1, Y_2, \dots, Y_n$  such that  $X_i \subseteq Y_i$ . Prove that the intersection of all the  $X_i$  is a subset of the intersection of all the  $Y_i$ :

$$\bigcap_{i=1}^n X_i \subseteq \bigcap_{i=1}^n Y_i$$

**Problem 34** Suppose that  $S_1, S_2, \dots, S_n$  are sets. Prove the following generalization of DeMorgan's laws:

$$(i) \left(\bigcap_{i=1}^n S_i\right)^c = \bigcup_{i=1}^n S_i^c, \text{ and}$$

$$(ii) \left(\bigcup_{i=1}^n S_i\right)^c = \bigcap_{i=1}^n S_i^c.$$

**Problem 35** Prove by induction that the Fibonacci number  $f_{4n}$  is a multiple of 3.

**Problem 36** Prove that if  $r$  is a real number  $r \neq 1$  and  $r \neq 0$  then

$$\sum_{i=0}^n r^i = \frac{1 - r^{n+1}}{1 - r}$$

**Problem 37** Prove by induction that the Fibonacci number  $f_{5n}$  is a multiple of 5.

**Problem 38** Prove by induction that the Fibonacci number  $f_n$  has the value

$$f_n = \frac{\sqrt{5}}{5} \cdot \left(\frac{1 + \sqrt{5}}{2}\right)^n - \frac{\sqrt{5}}{5} \cdot \left(\frac{1 - \sqrt{5}}{2}\right)^n$$

**Problem 39** Prove that for sufficiently large  $n$  the Fibonacci number  $f_n$  is the integer closest to

$$\frac{\sqrt{5}}{5} \left(\frac{1 + \sqrt{5}}{2}\right)^n$$

and compute the exact value of  $f_{30}$ . Show your work (i.e. don't look the result up on the net).

**Problem 40** Prove that  $\frac{n(n-1)(n-2)(n-3)}{24}$  is a whole number for any whole number  $n$ .

**Problem 41** Consider the statement "All cars are the same color." and the following "proof".

*Proof:*

We will prove for  $n \geq 1$  that for any set of  $n$  cars all the cars in the set have the same color.

- *Base Case:*  $n=1$  If there is only one car then clearly there is only one color the car can be.
- *Inductive Hypothesis:* Assume that for any set of  $n$  cars there is only one color.
- *Inductive step:* Look at any set of  $n + 1$  cars. Number them:  $1, 2, 3, \dots, n, n + 1$ . Consider the sets  $\{1, 2, 3, \dots, n\}$  and  $\{2, 3, 4, \dots, n + 1\}$ . Each is a set of only  $n$  cars, therefore for each set there is only one color. But the  $n^{\text{th}}$  car is in both sets so the color of the cars in the first set must be the same as the color of the cars in the second set. Therefore there must be only one color among all  $n + 1$  cars.
- The proof follows by induction.  $\square$

What are the problems with this proof?

## Functions

In this section we will define functions and extend much of our ability to work with sets to infinite sets. There are a number of different types of functions and so this section contains a great deal of terminology.

Recall that two finite sets are the same size if they contain the same number of elements. It is possible to make this idea formal by using functions and, once the notion is formally defined, it can be applied to infinite sets.

**Definition 16** An **ordered pair** is a collection of two elements with the added property that one element comes first and one element comes second. The set containing only  $x$  and  $y$  (for  $x \neq y$ ) is written  $\{x, y\}$ . The ordered pair containing  $x$  and  $y$  with  $x$  first is written  $(x, y)$ . Notice that while  $\{x, x\}$  is not a well defined set,  $(x, x)$  is a well defined ordered pair because the two copies of  $x$  are different by virtue of coming first and second.

The reason for defining ordered pairs at this point is that it permits us to make an important formal definition that pervades the rest of mathematics.

**Definition 17** A function  $f$  with domain  $S$  and range  $T$  is a set of ordered pairs  $(s, t)$  with first element from  $S$  and second element from  $T$  that has the property that every element of  $S$  appears exactly once as the first element in some ordered pair. We write  $f: S \rightarrow T$  for such a function.

**Example 15** Suppose that  $A = \{a, b, c\}$  and  $B = \{0, 1\}$  then

$$f = \{(a, 0), (b, 1), (c, 0)\}$$

is a function from  $A$  to  $B$ . The function  $f: A \rightarrow B$  can also be specified by saying  $f(a) = 0$ ,  $f(b) = 1$  and  $f(c) = 0$ .

The set of ordered pairs  $\{(a, 0), (b, 1)\}$  is not a function from  $A$  to  $B$  because  $c$  is not the first coordinate of any ordered pair. The set of ordered pairs  $\{(a, 0), (a, 1), (b, 0), (c, 0)\}$  is not a function from  $A$  to  $B$  because  $a$  appears as the first coordinate of two different ordered pairs.

In calculus you may have learned the *vertical line rule* that states that the graph of a function may not intersect a vertical line at more than one point. This corresponds to requiring that each point in the domain of the function appear in only one ordered pair. In set theory, all functions are required to state their domain and range when they are defined. In calculus functions had a domain that was a subset of the real numbers and you were sometimes required to identify the subset.

**Example 16** This example contrasts the way functions were treated in a typical calculus course with the way we treat them in set theory.

**Calculus:** find the domain of the function

$$f(x) = \sqrt{x}$$

Since we know that the square root function exists only for non-negative real numbers the domain is  $\{x : x \geq 0\}$ .

**Set theory:** the function  $f = \sqrt{x}$  from the non-negative real numbers to the real numbers is the set

of ordered pairs  $\{(r^2, r) : r \geq 0\}$ . This function is well defined because each non-negative real number is the square of some positive real number.

The major contrasts between functions in calculus and functions in set theory are:

- (i) The domain of functions in calculus are often specified only by implication (you have to know how all the functions used work) and are almost always a subset of the real numbers. The domain in set theory must be explicitly specified and may be any set at all.
- (ii) Functions in calculus typically had graphs that you could draw and look at. Geometric intuition driven by the graphs plays a major role in our understanding of functions. Functions in set theory are seldom graphed and often don't have a graph.

A point of similarity between calculus and set theory is that the range of the function is not explicitly specified. When we have a function  $f: S \rightarrow T$  then the range of  $f$  is a subset of  $T$ .

**Definition 18** If  $f$  is a function then we denote the domain of  $f$  by  $\text{dom}(f)$  and the range of  $f$  by  $\text{rng}(f)$

**Example 17** Suppose that  $f: \mathbb{N} \rightarrow \mathbb{N}$  is defined by  $f(n) = 2n$ . Then the domain and range of  $f$  are the integers:  $\text{dom}(f) = \text{rng}(f) = \mathbb{N}$ . If we specify the ordered pairs of  $f$  we get

$$f = \{(n, 2n) : n \in \mathbb{N}\}$$

There are actually two definitions of range that are used in mathematics. The definition we are using, the set from which second coordinates of ordered pairs in a function are drawn, is also the definition typically using in computer science. The other definition is the set of second coordinates that actually appear in ordered pairs. This set, which we will define formally later, is the *image* of the function. To make matters even worse the set we are calling the range of a function is also called the *co-domain*. We include these confusing terminological notes for students that may try and look up supplemental material.

**Definition 19** Let  $X, Y$ , and  $Z$  be sets. The **composition** of two functions  $f: X \rightarrow Y$  and  $g: Y \rightarrow Z$  is a function  $h: X \rightarrow Z$  for which  $h(x) = g(f(x))$  for all  $x \in X$ . We write  $g \circ f$  for the composition of  $g$  with  $f$ .

The definition of the composition of two functions requires a little checking to make sure it makes sense. Since every point must appear as a first coordinate of an ordered pair in a function, every result of applying  $f$  to an element of  $X$  is an element of  $Y$  to which  $g$  can be applied. This means that  $h$  is a well-defined set of ordered pairs. Notice that the order of composition is important - if the sets  $X, Y$ , and  $Z$  are distinct there is only one order in which composition even makes sense.

**Example 18** Suppose that  $f: \mathbb{N} \rightarrow \mathbb{N}$  is given by  $f(n) = 2n$  while  $g: \mathbb{N} \rightarrow \mathbb{N}$  is given by  $g(n) = n + 4$ . Then

$$(g \circ f)(n) = 2n + 4$$

while

$$(f \circ g)(n) = 2(n + 4) = 2n + 8$$

We now start a series of definitions that divide functions into a number of classes. We will arrive at a point where we can determine if the mapping of a function is reversible, if there is a function that exactly reverses the action of a given function.

**Definition 20** A function  $f: S \rightarrow T$  is **injective** or **one-to-one** if no element of  $T$  (no second coordinate) appears in more than one ordered pair. Such a function is called an **injection**.

**Example 19** The function  $f: \mathbb{N} \rightarrow \mathbb{N}$  given by  $f(n) = 2n$  is an injection. The ordered pairs of  $f$  are  $(n, 2n)$  and so any number that appears as a second coordinate does so once.

The function  $g: \mathbb{Z} \rightarrow \mathbb{Z}$  given by  $g(n) = n^2$  is not an injection. To see this notice that  $g$  contains the ordered pairs  $(1, 1)$  and  $(-1, 1)$  so that 1 appears twice as the second coordinate of an ordered pair.

**Definition 21** A function  $f: S \rightarrow T$  is **surjective** or **onto** if every element of  $T$  appears in an ordered pair. Surjective functions are called **surjections**.

We use the symbol  $\mathbb{R}$  for the real numbers. We also assume familiarity with interval notation for contiguous subsets of the reals. For real numbers  $a \leq b$

$$(a, b) \text{ is } \{x : a < x < b\}$$

$$[a, b) \text{ is } \{x : a \leq x < b\}$$

$$[a, b] \text{ is } \{x : a \leq x \leq b\}$$

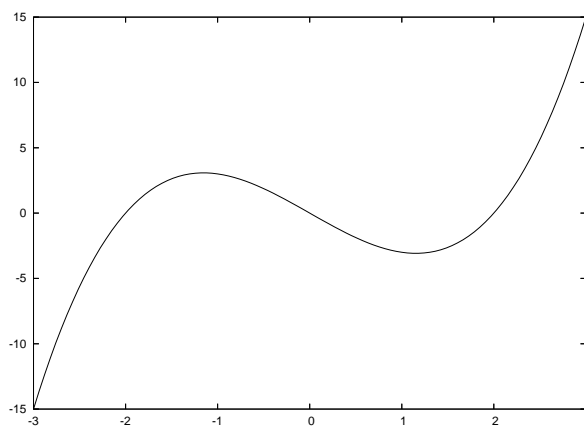
$$[a, b] \text{ is } \{x : a \leq x \leq b\}$$

**Example 20** The function  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  given by  $f(n) = 5 - n$  is a surjection. If we set  $m = 5 - n$  then  $n = 5 - m$ . This means that if we want to find some  $n$  so that  $f(n)$  is, for example, 8, then  $5 - 8 = -3$  and we see that  $f(-3) = 8$ . This demonstrates that all  $m$  have some  $n$  so that  $f(n) = m$ , showing that all  $m$  appear as the second coordinate of an ordered pair in  $f$ .

The function  $g: \mathbb{R} \rightarrow \mathbb{R}$  given by  $g(x) = \frac{x^2}{1+x^2}$  is not a surjection because  $-1 < g(x) < 1$  for all  $x \in \mathbb{R}$ .

**Definition 22** A function that is both surjective and injective is said to be **bijective**. Bijective functions are called **bijections**.

**Example 21** The function  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  given by  $f(n) = n$  is a bijection. All of its ordered pairs have the same first and second coordinate. This function is called the identity function.



The function  $g: \mathbb{R} \rightarrow \mathbb{R}$  given by  $g(x) = x^3 - 4x$  is not a bijection. It is not too hard to show that it is a surjection, but it fails to be an injection. The portion of the graph shown above demonstrates that  $g(x)$  takes on the same value more than once. This means that

some numbers appear twice as second coordinates of ordered pairs in  $g$ . We can use the graph because  $g$  is a function from the real numbers to the real numbers.

For a function  $f : S \rightarrow T$  to be a bijection every element of  $S$  appears in an ordered pair as the first member of an ordered pair and every element of  $T$  appears in an ordered pair as the second member of an ordered pair. Another way to view a bijection is as a matching of the elements of  $S$  and  $T$  so that every element of  $S$  is paired with an element of  $T$ . For finite sets this is clearly only possible if the sets are the same size and, in fact, this is the formal definition of “same size” for sets.

**Definition 23** Two sets  $S$  and  $T$  are defined to be the same size or to have equal cardinality if there is a bijection  $f : S \rightarrow T$ .

**Example 22** The sets  $A = \{a, b, c\}$  and  $Z = \{1, 2, 3\}$  are the same size. This is obvious because they have the same number of elements,  $|A| = |Z| = 3$  but we can construct an explicit bijection

$$f = \{(a, 3), (b, 1), (c, 2)\}$$

with each member of  $A$  appearing once as a first coordinate and each member of  $B$  appearing once as a second coordinate. This bijection is a witness that  $A$  and  $B$  are the same size.

Let  $E$  be the set of even integers. Then the function

$$g : \mathbb{Z} \rightarrow E$$

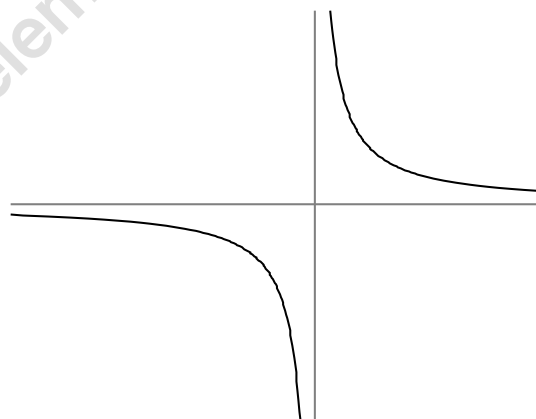
in which  $g(n) = 2n$  is a bijection. Notice that each integer can be put into  $g$  and that each even integer has exactly one integer that can be doubled to make it. The existence of  $g$  is a witness that the set of integers and the set of even integers are the same size. This may seem a bit bizarre because the set  $\mathbb{Z} - E$  is the infinite set of odd integers. In fact one hallmark of an infinite set is that it can be the same size as a proper subset. This also means we now have an equality set for sizes of infinite sets. We will do a good deal more with this in Chapter 3.

Bijections have another nice property: they can be unambiguously reversed.

**Definition 24** The inverse of a function  $f : S \rightarrow T$  is a function  $g : T \rightarrow S$  so that for all  $x \in S$ ,  $g(f(x)) = x$  and for all  $y \in T$ ,  $f(g(y)) = y$ .

If a function  $f$  has an inverse we use the notation  $f^{-1}$  for that inverse. Since an exponent of  $-1$  also means reciprocal in some circumstances this can be a bit confusing. The notational confusion is resolved by considering context. So long as we keep firmly in mind that functions are sets of ordered pairs it is easy to prove the proposition/definition that follows after the next example.

**Example 23** If  $E$  is the set of even integers then the bijection  $f(n) = 2n$  from  $\mathbb{Z}$  to  $E$  has the inverse  $f^{-1} : E \rightarrow \mathbb{Z}$  given by  $g(2n) = n$ . Notice that defining the rule for  $g$  as depending on the argument  $2n$  seamlessly incorporates the fact that the domain of  $g$  is the even integers.



If  $g(x) = \frac{x}{x-1}$ , shown above with its asymptotes  $x = 1$  and  $y = 1$  then  $f$  is a function from the set  $H = \mathbb{R} - \{1\}$  to itself. The function was chosen to have asymptotes at equal  $x$  and  $y$  values; this is a bit unusual. The function  $g$  is a bijection. Notice that the graph intersects any horizontal or vertical line in at most one point. Every value except  $x = 1$  may be put into  $g$  meaning that  $g$  is a function on  $H$ . Since the vertical asymptote goes off to  $\infty$  in both directions, all values in  $H$  come out of  $g$ . This demonstrates  $g$  is a bijection. This means that it has an inverse which we now compute using a standard



## FUNCTIONS

technique from calculus classes.

$$\begin{aligned} y &= \frac{x}{x-1} \\ y(x-1) &= x \\ xy - y &= x \\ xy - x &= y \\ x(y-1) &= y \\ x &= \frac{y}{y-1} \end{aligned}$$

which tells us that  $g^{-1}(x) = \frac{x}{x-1}$  so  $g = g^{-1}$ : the function is its own inverse.

**Proposition 5** A function has an inverse if and only if it is a bijection.

Proof:

Suppose that  $f : S \rightarrow T$  is a bijection. Then if  $g : T \rightarrow S$  has ordered pairs that are the exact reverse of those given by  $f$  it is obvious that for all  $x \in S$ ,  $g(f(x)) = x$ , likewise that for all  $y \in T$ ,  $f(g(y)) = y$ . We have that bijections possess inverses. It remains to show that non-bijections do not have inverses.

If  $f : S \rightarrow T$  is not a bijection then either it is not a surjection or it is not an injection. If  $f$  is not a surjection then there is some  $t \in T$  that appears in no ordered pair of  $f$ . This means that no matter what  $g(t)$  is,  $f(g(t)) \neq t$  and we fail to have an inverse. If, on the other hand,  $f : S \rightarrow T$  is a surjection but fails to be an injection then for some distinct  $a, b \in S$  we have that  $f(a) = t = f(b)$ . For  $g : T \rightarrow S$  to be an inverse of  $f$  we would need  $g(t) = a$  and  $g(t) = b$ , forcing  $t$  to appear as the first coordinate of two ordered pairs in  $g$  and so rendering  $g$  a non-function. We thus have that non-bijections do not have inverses.  $\square$

The type of inverse we are discussing above is a *two-sided inverse*. The functions  $f$  and  $f^{-1}$  are mutually inverses of one another. It is possible to find a function that is a one-way inverse of a function so that  $f(g(x)) = x$  but  $g(f(x))$  is not even defined. These are called *one-sided inverses*.

Note on mathematical grammar: Recall that when two notions, such as “bijection” and “has an inverse” are equivalent we use the phrase “if and only if” (abbreviated iff) to phrase a proposition declaring that the notions are equivalent. A proposition that  $A$  iff

$B$  is proven by first assuming  $A$  and deducing  $B$  and then separately assuming  $B$  and deducing  $A$ . The formal symbol for  $A$  iff  $B$  is  $A \Leftrightarrow B$ . Likewise we have symbols for the ability to deduce  $B$  given  $A$ ,  $A \Rightarrow B$  and vice-versa  $B \Rightarrow A$ . These symbols are spoken “ $A$  implies  $B$ ” and “ $B$  implies  $A$ ” respectively.

**Proposition 6** Suppose that  $X, Y$ , and  $Z$  are sets. If  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  are bijections then so is  $g \circ f : X \rightarrow Z$ .

Proof: this proof is left as an exercise.

**Definition 25** Suppose that  $f : A \rightarrow B$  is a function. The **image of  $A$  in  $B$**  is the subset of  $B$  made of elements that appear as the second element of ordered pairs in  $f$ . Colloquially the image of  $f$  is the set of elements of  $B$  hit by  $f$ . We use the notation  $Im(f)$  for images. In other words  $Im(f) = \{f(a) : a \in A\}$ .

**Example 24** If  $f : \mathbb{N} \rightarrow \mathbb{N}$  is given by the rule  $f(n) = 3n$  then the set  $T = \{0, 3, 6, \dots\}$  of natural numbers that are multiples of three is the image of  $f$ . Notation:  $Im(f) = T$ .

If  $g : \mathbb{R} \rightarrow \mathbb{R}$  given by  $g(x) = x^2$  then

$$Im(g) = \{y : y \geq 0, y \in \mathbb{R}\}$$

There is a name for the set of all ordered pairs drawn from two sets.

**Definition 26** If  $A$  and  $B$  are sets then the set of all ordered pairs with the first element from  $A$  and the second from  $B$  is called the **Cartesian Product** of  $A$  and  $B$ .

The notation for the Cartesian product of  $A$  and  $B$  is  $A \times B$ . using curly brace notation:

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

**Example 25** If  $A = \{1, 2\}$  and  $B = \{x, y\}$  then

$$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$$

The **Cartesian plane** is an example of a Cartesian product of the real numbers with themselves:  $\mathbb{R} \times \mathbb{R}$ .

## Permutations

In this section we will look at a very useful sort of function, bijections of finite sets.

**Definition 2.27** A **permutation** is a bijection of a finite set with itself. Likewise a bijection of a finite set  $X$  with itself is called a **permutation of  $X$** .

**Example 2.26** Let  $A = \{a, b, c\}$  then the possible permutations of  $A$  consist of the following six functions:

$$\begin{aligned} \{(a, a)(b, b)(c, c)\} & \quad \{(a, a)(b, c)(c, b)\} \\ \{(a, b)(b, a)(c, c)\} & \quad \{(a, b)(b, c)(c, a)\} \\ \{(a, c)(b, a)(c, b)\} & \quad \{(a, c)(b, b)(c, a)\} \end{aligned}$$

Notice that the number of permutations of three objects does not depend on the identity of those objects. In fact there are always six permutations of any set of three objects. We now define a handy function that uses a rather odd notation. The method of showing permutations in Example 2.26, explicit listing of ordered pairs, is a bit cumbersome.

**Definition 2.8** Assume that we have agreed on an order, e.g.  $a, b, c$ , for the members of a set  $X = \{a, b, c\}$ . Then **one-line notation** for a permutation  $f$  consists of listing the first coordinate of the ordered pairs in the agreed on order. The table in Example 2.26 would become:

abc	acb
bac	bca
cab	cba

in one line notation. Notice the saving of space. **Definition 2.9** The **factorial** of a natural number  $n$  is the product

$$n(n-1)(n-2)\cdots 3\cdot 2\cdot 1 = \prod_{i=1}^n i$$

with the convention that the factorial of 0 is 1. We denote the factorial of  $n$  as  $n!$ , spoken "n factorial".

**Example 2.7** Here are the first few factorials:

$n$	0	1	2	3	4	5	6	7
$n!$	1	1	2	6	24	120	720	5040

**Proposition 7** The number of permutations of a finite set with  $n$  elements is  $n!$ .

Proof: this proof is left as an exercise.

Notice that one implication of Proposition 2.6 is that the composition of two permutations is a permutation. This means that the set of permutations of a set is *closed* under functional composition.

**Definition 3.0** A **fixed point** of a function  $f: S \rightarrow S$  is any  $x \in S$  such that  $f(x) = x$ . We say that  $f$  **fixes  $x$** .

## Problems

**Problem 4.2** Suppose for finite sets  $A$  and  $B$  that  $f: A \rightarrow B$  is an injective function. Prove that

$$|B| \geq |A|$$

**Problem 4.3** Suppose that for finite sets  $A$  and  $B$  that  $f: A \rightarrow B$  is a surjective function. Prove that  $|A| \geq |B|$ .

**Problem 4.4** Using functions from the integers to the integers give an example of

- (i) A function that is an injection but not a surjection.
- (ii) A function that is a surjection but not an injection.
- (iii) A function that is neither an injection nor a surjection.
- (iv) A bijection that is not the identity function.

**Problem 4.5** For each of the following functions from the real numbers to the real numbers say if the function is surjective or injective. It may be neither.

- (i)  $f(x) = x^2$  (ii)  $g(x) = x^3$
- (iii)  $h(x) = \begin{cases} \sqrt{x} & x \geq 0 \\ -\sqrt{-x} & x < 0 \end{cases}$

## *Interlude*

### **The Collatz Conjecture**

One of the most interesting features of mathematics is that it is possible to phrase problems in a few lines that turn out to be incredibly hard. The Collatz conjecture was first posed in 1937 by Lothar Collatz. Define the function  $f$  from the natural numbers to the natural numbers with the rule

$$f(n) = \begin{cases} 3n + 1 & n \text{ odd} \\ \frac{n}{2} & n \text{ even} \end{cases}$$

Collatz' conjecture is that if you apply  $f$  repeatedly to a positive integer then the resulting sequence of numbers eventually arrives at one. If we start with 17, for example, the result of repeatedly applying  $f$  is:

$$f(17) = 52, f(52) = 26, f(26) = 13, f(13) = 40, f(40) = 20, f(20) = 10,$$

$$f(10) = 5, f(5) = 16, f(16) = 8, f(8) = 4, f(4) = 2, f(2) = 1$$

The sequences of numbers generated by repeatedly applying  $f$  to a natural number are called *hailstone sequences* with the collapse of the value when a large power of 2 appears being analogous to the impact of a hailstone. If we start with the number 27 then 111 steps are required to reach one and the largest intermediate number is 9232. This quite irregular behavior of the sequence is not at all apparent in the original phrasing of the problem.

The Collatz conjecture has been checked for numbers up to  $5 \times 2^{61}$  (about  $5.764 \times 10^{18}$ ) by using a variety of computational tricks. It has not, however, been proven or disproven. The very simple statement of the problem causes mathematicians to underestimate the difficulty of the problem. At one point a mathematician suggested that the problem might have been developed by the Russians as a way to slow American mathematical research. This was after several of his colleagues spent months working on the problem without obtaining results.

A simple (but incorrect) argument suggests that hailstone sequences ought to grow indefinitely. Half of all numbers are odd, half are even. The function  $f$  slightly more than triples odd numbers and divides even numbers in half. Thus, on average,  $f$  increases the value of numbers. The problem is this: half of all even numbers are multiples of four and so are divided in half twice. One-quarter of all even numbers are multiples of eight and so get divided in half three times, and so on. The net effect of factors that are powers of two is to defeat the simple argument that  $f$  grows "on average".

## CHAPTER 2. BASIC SET THEORY

**Problem 46** True or false (and explain): The function  $f(x) = \frac{x-1}{x+1}$  is a bijection from the real numbers to the real numbers.

**Problem 47** Find a function that is an injection of the integers into the even integers that does not appear in any of the examples in this chapter.

**Problem 48** Suppose that  $B \subset A$  and that there exists a bijection  $f: A \rightarrow B$ . What may be reasonably deduced about the set  $A$ ?

**Problem 49** Suppose that  $A$  and  $B$  are finite sets. Prove that  $|A \times B| = |A| \cdot |B|$ .

**Problem 50** Suppose that we define  $h: \mathbb{N} \rightarrow \mathbb{N}$  as follows. If  $n$  is even then  $h(n) = n/2$  but if  $n$  is odd then  $h(n) = 3n + 1$ . Determine if  $h$  is a (i) surjection or (ii) injection.

**Problem 51** Prove proposition 2.6.

**Problem 52** Prove or disprove: the composition of injections is an injection.

**Problem 53** Prove or disprove: the composition of surjections is a surjection.

**Problem 54** Prove proposition 2.7.

**Problem 55** List all permutations of

$$X = \{1, 2, 3, 4\}$$

using one-line notation.

**Problem 56** Suppose that  $X$  is a set and that  $f, g$ , and  $h$  are permutations of  $X$ . Prove that the equation  $f \circ g = h$  has a solution  $g$  for any given permutations  $f$  and  $h$ .

**Problem 57** Examine the permutation  $f$  of  $Q = \{a, b, c, d, e\}$  which is **bcade** in one line notation. If we create the series  $f, f \circ f, f \circ (f \circ f), \dots$  does the identity function, **abcde**, ever appear in the series? If so, what is its first appearance? If not, why not?

**Problem 58** If  $f$  is a permutation of a finite set, prove that the sequence  $f, f \circ f, f \circ (f \circ f), \dots$  must contain repeated elements.

**Problem 59** Suppose that  $X$  and  $Y$  are finite sets and that  $|X| = |Y| = n$ . Prove that there are  $n!$  bijections of  $X$  into  $Y$ .

**Problem 60** Suppose that  $X$  and  $Y$  are sets with  $|X| = n, |Y| = m$ . Count the number of functions from  $X$  to  $Y$ .

**Problem 61** Suppose that  $X$  and  $Y$  are sets with  $|X| = n, |Y| = m$  for  $m > n$ . Count the number of injections of  $X$  into  $Y$ .

**Problem 62** For a finite set  $S$  with a subset  $T$  prove that the permutations of  $S$  that have all members of  $T$  as fixed points form a set that is closed under functional composition.

**Problem 63** Compute the number of permutations of a set  $S$  with  $n$  members that fix at least  $m < n$  points.

**Problem 64** Using any technique at all, estimate the fraction of permutations of an  $n$ -element set that have no fixed points. This problem is intended as an exploration.

**Problem 65** Let  $X$  be a finite set with  $|X| = n$ . Let  $C = X \times X$ . How many subsets of  $C$  have the property that every element of  $X$  appears once as a first coordinate of some ordered pair and once as a second coordinate of some ordered pair?

**Problem 66** An alternate version of Sigma ( $\sum$ ) and Pi ( $\prod$ ) notation works by using a set as an index. If  $S = \{1, 3, 5, 7\}$  then

$$\sum_{s \in S} s = 16 \quad \text{and} \quad \prod_{s \in S} s = 105$$

$$s \in S$$

$$s \in S$$

Given all the material so far, give and defend reasonable values for the sum and product of an empty set.

**Problem 67** Suppose that  $f_\alpha: [0, 1] \rightarrow [0, 1]$  for  $-1 < \alpha < \infty$  is given by

$$f_\alpha(x) = \frac{(\alpha + 1)x}{\alpha x + 1},$$

prove that  $f_\alpha$  is a bijection.

**Problem 68** Find, to five decimals accuracy:

$$\ln(200!)$$

Explain how you obtained the answer.

$$\infty + 1$$

$$\infty + 1$$

We conclude the chapter with a brief section that demonstrates a strange thing that can be accomplished with set notation. We choose to represent the natural numbers  $0, 1, 2, \dots$  by sets that contain the number of elements counted by the corresponding natural number. We also choose to do so as simply as possible, using only curly braces and commas. Given this the numbers and their corresponding sets are:

$$\begin{aligned} 0 &: \{\} \\ 1 &: \{\{\}\} = \{0\} \\ 2 &: \{\{\}, \{\{\}\}\} = \{0, 1\} \\ 3 &: \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\} = \{0, 1, 2\} \\ 4 &: \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}\} \\ &= \{0, 1, 2, 3\} \end{aligned}$$

The trick for the above representation is this. Zero is represented by the empty set. One is represented by the set of the only thing we have constructed - zero, represented as the empty set. Similarly the representation of two is the set of the representation of zero and one (the empty set and the set of the empty set). This representation is incredibly inefficient but it uses a very small number of symbols. This representation also has a useful property. As always, we will start with a definition.

**Definition 31** *The minimal set representation of the natural numbers is constructed as follows:*

- (i) *Let 0 be represented by the empty set.*
- (ii) *For  $n > 0$  let  $n$  be represented by the set  $\{0, 1, \dots, n - 1\}$ .*

The shorthand  $\{0, 1\}$  for  $\{\{\}, \{\{\}\}\}$  is called the *simplified notation* for the minimal set representation. We now give the useful property of the minimal set representation.

**Proposition 8**  $n + 1 = n \cup \{n\}$

Proof:

This follows directly from Definition 2.31 by considering the set difference of the representations of  $n$  and  $n - 1$ .  $\square$

The definition says that any set of the representations of consecutive natural numbers, starting at zero, is

the representation of the next natural number. This permits us to conclude that the set of all natural numbers

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

fits the definition of a natural number. Which natural number is it? It is easy to see, in the minimal set representation, that for natural numbers  $m$  and  $n$ ,  $m < n$  implies that the representation of  $m$  is a subset of the representation of  $n$ . Every finite natural number is a subset of the set of all natural numbers and so we conclude that  $\{0, 1, 2, \dots\}$  is an infinite natural number. The set notation thus permits us to construct an infinite number.

The set consisting of the representations of all finite natural numbers is an infinite natural number. The number has been given the name  $\omega$ , the lower-case omega. In addition to being a letter omega traditionally also means “the last”. The number  $\omega$  comes after all the finite natural numbers. If we now apply Proposition 2.8 we see that

$$\omega \cup \{\omega\} = \omega + 1$$

This means that we can add one to an infinite number. Is the resulting number  $\omega + 1$  a different number from  $\omega$ ? It turns out the answer is “yes”, because the representations of these numbers are different as sets.

*Interlude***Russell's Paradox**

**Bertrand Arthur William Russell, 3rd Earl Russell, OM, FRS (18 May 1872-2 February 1970), commonly known as simply Bertrand Russell, was a British philosopher, logician, mathematician, historian, religious skeptic, social reformer, socialist and pacifist. Although he spent the majority of his life in England, he was born in Wales, where he also died.**



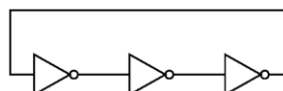
Let  $Q$  be the set of all sets that do not contain themselves as a member. Consider the question: "Does  $Q$  contain itself?" If the answer to this question is no then  $Q$ , by definition must contain itself. If, however,  $Q$  contains itself then it is by definition unable to contain itself. This rather annoying contradiction, constructed by Russell, had a rather amusing side effect.

Friedrich Frege had just finished the second of a three volume set of works called the *Basic Laws of Arithmetic* that was supposed to remove all intuition from mathematics and place it on a purely logical basis. Russell wrote Frege, explaining his paradox. Frege added an appendix to his second volume that attempted to avoid Russell's paradox. The third volume was never published.

It is possible to resolve Russell's paradox by being much more careful about what objects may be defined to be sets; the *category* of all sets that do not contain themselves gives rise to no contradiction (it does give rise to an entire field of mathematics, category theory). The key to resolving the paradox from a set theoretic perspective is that one cannot assume that, for every property, there is a set of all things satisfying that property. This is a reason why it is important that a set is properly defined. Another consequence of Russell's paradox is a warning that self-referential statements are both potentially interesting and fairly dangerous, at least on the intellectual plane.

The original phrasing of Russell's paradox was in terms of normal and abnormal sets. A set is *normal* if it fails to contain itself and abnormal otherwise. Consider the set of all normal sets. If this set is abnormal, it contains itself but by definition the set contains only normal sets and hence it is itself normal. The normality of this set forces the set to contain itself, which makes it abnormal. This is simply a rephrasing of the original contradiction.

Puzzle: what does the circuit below have to do with Russell's paradox and what use is it?



# Basic properties of the integers

## Definitions

The **natural numbers** are the numbers  $1, 2, 3, \dots$  (some authors include zero, as well), and for shorthand, we will denote the collection of them by  $\mathbf{N}$ . The **integers** (a.k.a. the **whole numbers**) are the natural numbers, together with zero and the negatives of the natural numbers, and we will denote them by  $\mathbf{Z}$ . So,

$$\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

The integers come equipped with extra structure with which you are all familiar: addition (+), multiplication ( $\cdot$ ), and an ordering ( $<$ ). I'll leave addition and multiplication undefined (but I could define it by starting from even more basic assumptions). As for ordering, I'll simply point out that one can give the following definition:

**Definition 1.1.** Given two integers  $a, b$ , we say that  $a$  is **less than**  $b$ , written  $a < b$ , if there exists a  $c \in \mathbf{N}$  such that

$$b = a + c.$$

## 2 Basic properties of the integers

In this section, we'll list some basic properties of the integers that will form the basis of everything we will prove this semester, i.e. everything we prove this semester will be traceable all the way back to these simple properties. In the next section, we will prove some basic consequences of these properties; you will prove more basic consequences on your first assignment.

### 1 Arithmetic properties

We begin with the *arithmetic* properties, i.e. those related to addition, multiplication, and the relation between the two.

- (1) if  $a, b \in \mathbf{Z}$ , then  $a + b \in \mathbf{Z}$  (closure under addition)
- (2) if  $a, b \in \mathbf{Z}$ , then  $a \cdot b \in \mathbf{Z}$  (closure under multiplication)
- (3) if  $a, b \in \mathbf{Z}$ , then  $a + b = b + a$  (commutativity of addition)
- (4) if  $a, b \in \mathbf{Z}$ , then  $a \cdot b = b \cdot a$  (commutativity of multiplication)
- (5) if  $a, b, c \in \mathbf{Z}$ , then  $a + (b + c) = (a + b) + c$  (associativity of addition)
- (6) if  $a, b, c \in \mathbf{Z}$ , then  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  (associativity of multiplication)
- (7) there exists an element  $0 \in \mathbf{Z}$  such that for all  $a \in \mathbf{Z}$

$$a + 0 = a \quad (\text{existence of an additive identity})$$

- (8) there exists an element  $1 \in \mathbf{Z}$  such that for all  $a \in \mathbf{Z}$

$$a \cdot 1 = a \quad (\text{existence of a multiplicative identity})$$

- (9) for every  $a \in \mathbf{Z}$ , there is a solution  $x \in \mathbf{Z}$  to

$$a + x = 0$$

(namely  $x = -a$ ) (existence of an additive inverse)

- (10) if  $a, b, c \in \mathbf{Z}$  and  $c \neq 0$ , then

$$a \cdot c = b \cdot c \text{ implies } a = b \quad (\text{cancellation law})$$

- (11) if  $a, b, c \in \mathbf{Z}$ , then  $a \cdot (b + c) = a \cdot b + a \cdot c$ . (distributivity law)

### Remark

- (a) For properties (1)–(8), there is a property of addition followed by a corresponding property of multiplication. This breaks down for property (9). The corresponding property would be that for all  $a \in \mathbf{Z}$  there is a solution  $x \in \mathbf{Z}$  to  $a \cdot x = 1$ . But, of course, this fails, e.g. take  $a = 2$ , there is no integer  $x$  such that  $2x = 1$ . However, the cancellation law (10) often serves as a substitute for the lack of multiplicative inverses: often you just want to divide both sides of an equation by the same quantity, the cancellation law allows you to do this without actually having to divide.



(b) Property (9) allows us to define **subtraction** as follows:

$$a - b := a + (-b),$$

i.e. subtracting  $b$  is *defined* to be adding its additive inverse.

## Ordering properties

The *ordering* properties are those concerning the relation  $<$ .

(12) if  $a, b > 0$ , then  $a + b > 0$  (closure of “ $> 0$ ” under addition)

(13) if  $a, b > 0$ , then  $a \cdot b > 0$  (closure of “ $> 0$ ” under multiplication)

(14) for any two integers  $a, b \in \mathbf{Z}$

exactly one of  $a < b$ ,  $a = b$ , or  $a > b$  is true (trichotomy law)

(15) Every non-empty set of natural numbers has a least element, i.e. for any  $S \subseteq \mathbf{N}$ , if  $S \neq \emptyset$ , then there is an  $m \in S$  such that

$m \leq s$ , for all  $s \in S$ . (well-ordering property)

### Remark

(a) Just to be clear, we write  $a > b$  if  $b < a$ , and we write  $a \leq b$  if  $a < b$  or  $a = b$ .

(b) Property (14) suggests a convenient way to prove two numbers  $a, b$  are equal: first prove  $a \leq b$ , then prove  $b \leq a$ . Since it can't be true that both  $a < b$  and  $b < a$ , this implies that  $a = b$ .

## 3 Some basic consequences

Here, we give some examples of some basic consequences of the properties listed above, as well as their proof. A major reason for including some proofs here is to give you some experience with proofs, so do read through them and try to understand why they are how they are. You'll have a chance to practice similar proofs on the first assignment.

**Proposition 3** *The additive identity in  $\mathbf{Z}$  is unique, i.e. 0 is the only element in  $\mathbf{Z}$  satisfying property (7).*

*Proof.* Let  $e \in \mathbf{Z}$  denote an integer such that  $a + e = a$  for all  $a \in \mathbf{Z}$ . In particular, this is true for  $a = 0$ , so

$$0 + e = 0.$$

Also,

$$\begin{aligned} 0 + e &= e + 0 && \text{(by commutativity of +)} \\ &= e. && \text{(since 0 is an additive identity)} \end{aligned}$$

Putting these together, we get

$$0 = 0 + e = e$$

so  $e = 0$ . So, any integer satisfying property (7) is necessarily 0.  $\square$

Can you find a shorter proof of the above?

**Proposition 3** *Given  $a \in \mathbf{Z}$ , its additive inverse is unique, i.e. the equation  $a + x = 0$  has a unique solution  $x \in \mathbf{Z}$ .*

*Proof.* Suppose  $x, y \in \mathbf{Z}$  are such that  $a + x = 0$  and  $a + y = 0$ . Adding  $x$  to both sides of the second equation gives

$$a + y + x = x.$$

By commutativity of addition, definition of  $x$ , and the fact that 0 is the additive identity,

$$a + y + x = a + x + y = 0 + y = y.$$

Combing these two lines gives  $x = y$ .  $\square$

**Proposition 3** *For all  $a \in \mathbf{Z}$ ,*

$$0 \cdot a = 0.$$

*Proof.* By distributivity,

$$(0 + 0) \cdot b = 0 \cdot b + 0 \cdot b.$$

Since 0 is an additive identity,  $0 + 0 = 0$ , so

$$(0 + 0) \cdot b = 0 \cdot b.$$

Combing these two equations yields

$$0 \cdot b + 0 \cdot b = 0 \cdot b.$$

Adding  $-(0 \cdot b)$  to both sides gives

$$0 \cdot b = 0,$$

as desired. □

**Proposition** For all  $a \in \mathbf{Z}$ ,

$$-a = (-1) \cdot a.$$

*Proof.* First, we'll show that  $(-1) \cdot a$  is an additive inverse of  $a$ . Indeed,

$$\begin{aligned} a + (-1) \cdot a &= 1 \cdot a + (-1) \cdot a && \text{(by (8) and (4))} \\ &= (1 + (-1)) \cdot a && \text{(by distributivity and (3))} \\ &= 0 \cdot a && \text{(by (7))} \\ &= 0, && \text{(by proposition 3.3)} \end{aligned}$$

as desired. By the uniqueness of additive inverses (proposition 3.2), the result follows. □

**Proposition** Let  $a, b \in \mathbf{Z}$ . If  $a \cdot b = 0$ , then  $a = 0$  or  $b = 0$ .

*Proof.* (Proof by contradiction) Since  $a \cdot b = 0$ ,

$$a \cdot b + a \cdot b = a \cdot b = 0.$$

By the uniqueness of additive inverses (proposition 3.2), this implies that

$$-(a \cdot b) = a \cdot b.$$

Applying proposition 3.4 (and (8)), gives

$$(-1) \cdot a \cdot b = 1 \cdot a \cdot b.$$

If  $b \neq 0$ , we can use the cancellation law to obtain

$$(-1) \cdot a = 1 \cdot a.$$

If  $a$  is also not 0, we can apply the cancellation law again to get

$$-1 = 1.$$

But  $1+1 = 2 \in \mathbf{N}$  and hence  $1+1 \neq 0$ , i.e.  $1 \neq -1$ . Therefore, the assumption that both  $a$  and  $b$  are not zero leads to a contradiction. Therefore, one of them must be zero, as desired.  $\square$

**Proposition** *Let  $b \in \mathbf{Z}$ . Then  $b \in \mathbf{N}$  if, and only,  $b > 0$ .*

*Proof.* ( $\Rightarrow$ ): suppose  $b \in \mathbf{N}$ . By (7) and (3),

$$b = 0 + b,$$

i.e., using definition 1.1 (with  $a = 0$  and  $c = b$ ), we can say  $0 < b$ .

( $\Leftarrow$ ): (contrapositive) suppose  $b \notin \mathbf{N}$ , then we want to show that  $b > 0$  is not true. By definition,  $\mathbf{Z}$  consists of the natural numbers, 0, and the negatives of the natural numbers. Since  $b \notin \mathbf{N}$ , either  $b = 0$  or there is  $a \in \mathbf{N}$  such that  $b = -a$ . If  $b = 0$ , then the trichotomy law implies that you can't have  $b > 0$ . In the second case ( $b = -a$ ), we have

$$0 = -a + a = b + a.$$

In terms of definition 1.1, this means that  $b < 0$ . By the trichotomy law,  $b > 0$  cannot be true.  $\square$

The well-ordering property is a statement about  $\mathbf{N}$ . More generally, given any “ordered set”  $X$ , we say it is “well-ordered” if every non-empty subset  $S \subseteq X$  has a least element. Let  $a \in \mathbf{Z}$  and define the notation

$$\mathbf{Z}_{\geq a} := \{b \in \mathbf{Z} : b \geq a\};$$

in particular,  $\mathbf{N} = \mathbf{Z}_{\geq 1}$ . All of these sets are well-ordered.

**Proposition** *Let  $a \in \mathbf{Z}$ , then  $\mathbf{Z}_{\geq a}$  is well-ordered.*

*Proof.* Let  $S \subseteq \mathbf{Z}_{\geq a}$  be any non-empty subset. Let

$$X := \{s - a + 1 : s \in S\}.$$

**Claim (1).**  *$X$  is a non-empty subset of  $\mathbf{N}$ .*

*Proof of claim (1).*  $X$  is non-empty since  $a - a + 1 = 1 \in X$ . To show  $X \subseteq \mathbf{N}$ , it's enough to show that for all  $x \in X$ ,  $x > 0$  (by proposition [3.6](#)). By a question on assignment 1,

$$s \geq a \text{ if, and only if, } s + r \geq a + r \text{ for all } r \in \mathbf{Z}. \quad (*)$$

Using this with  $r = -a + 1$ , we get that for all  $s \in S$

$$s - a + 1 \geq a - a + 1 = 1.$$

Let  $x \in X$ , then there is an  $s \in S$  such that  $x = s - a + 1$ . Hence,  $x \geq 1$ . □

Since  $\mathbf{N}$  is well-ordered and  $X$  is a non-empty subset of it, there is a least element  $x_0 \in X$ .

**Claim (2).**  $s_0 := x_0 + a - 1$  is a least element of  $S$ .

*Proof of claim (2).* Let  $s \in S$ . Using  $(*)$  again with  $r = -a + 1$ ,

$$s \geq s_0 \text{ if, and only if } s - a + 1 \geq x_0.$$

By definition of  $X$ ,  $s - a + 1 \in X$ , so we know that  $s - a + 1 \geq x_0$ . Hence,  $s \geq s_0$ , and the latter is a least element of  $S$ . □

$S$  was arbitrary, so  $\mathbf{Z}_{\geq a}$  is well-ordered. **Proposition** □

**3** *The integers  $\mathbf{Z}$  are not well-ordered.*

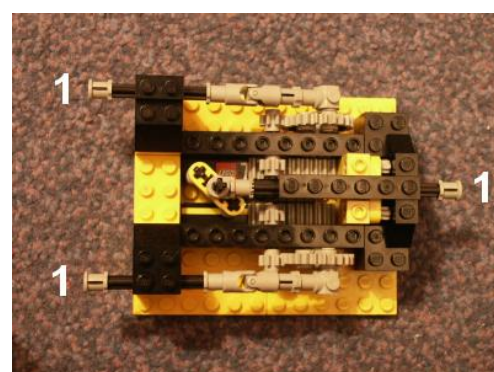
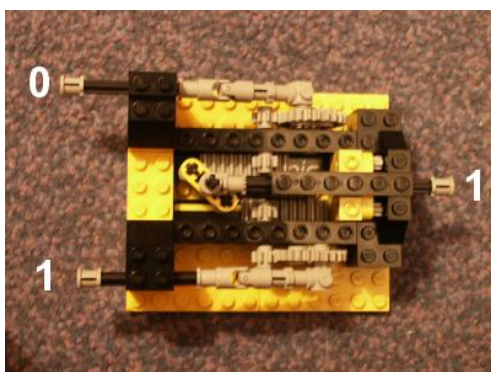
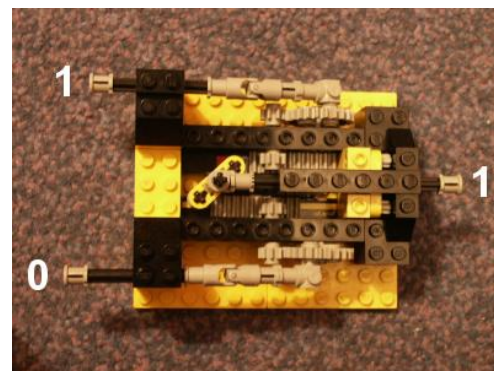
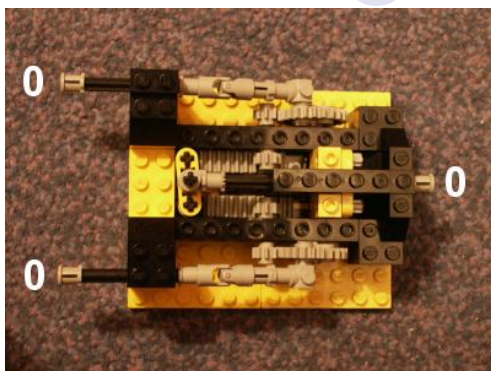
*Proof.* (Proof by counterexample) We need to find a non-empty subset  $S$  of  $\mathbf{Z}$  which has no least element. Let's simply take  $S = \mathbf{Z}$  (our proposed counterexample). Let's suppose  $m \in \mathbf{Z}$  is a least element and derive a contradiction. Since  $m = (m - 1) + 1$ , definition [1.1](#) says  $m - 1 < m$ , contradicting the minimality of  $m$ . Therefore,  $S = \mathbf{Z}$  has no least element. □

# UNIT 2



28

## §2 Boolean Algebra



29

# Outline

- Introduction
- Basic operations
- Boolean expressions and truth tables
- Basic theorems
- Commutative, associative, and distributive laws
- Simplification theorems
- Multiplying out and factoring
- DeMorgan's laws

30

# Introduction

- Boolean algebra is the mathematical foundation of logic design
  - George Boole (1847)
    - logic + algebra  $\rightarrow$  Boolean algebra
  - Claude Shannon (1939)
    - Boolean algebra  $\leftrightarrow$  logic design



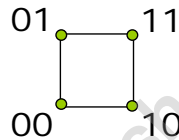
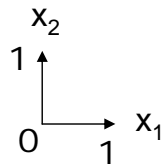
31

# Introduction

- Boolean (switching) variable  $x \in \{0,1\}$ 
  - 0, 1 are abstract symbols
    - They may correspond to {false, true} in logic, {off, on} of a switch, {low voltage, high voltage} of a CMOS circuit, or other meanings
- Boolean space  $\{0,1\}^n$ 
  - The configuration space of all possible  $\{0,1\}$  assignments to  $n$  Boolean variables

E.g.,

the Boolean space spanned by  $(x_1, x_2)$  is  $\{0,1\}^2 = \{0,1\} \times \{0,1\} = \{00, 01, 10, 11\}$

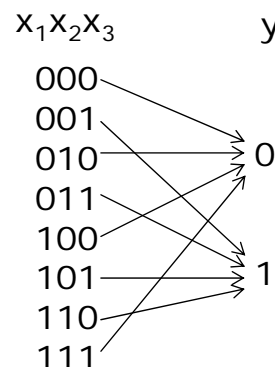
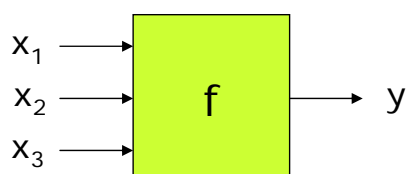


32

# Introduction

- Boolean function  $f(x_1, x_2, \dots, x_n)$  is a mapping:  $\{0,1\}^n \rightarrow \{0,1\}$ , where  $x_i$ 's are Boolean variables

E.g.,



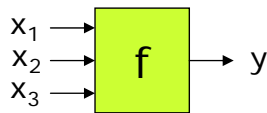
How many Boolean functions of  $n$  variables are there?

33



# Introduction

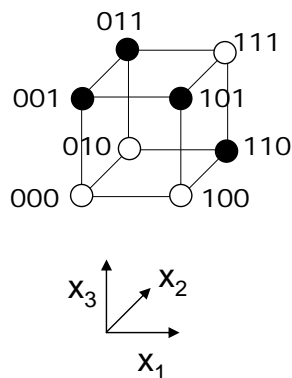
- There are many different ways to represent a Boolean function
  - E.g., truth tables, Boolean expressions (formulas), logic circuits, Binary Decision Diagrams, combinatorial cubes, ...



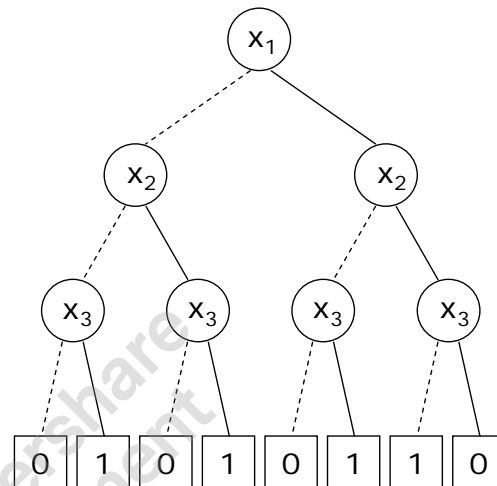
Truth table

$x_1x_2x_3$	$y$
000	0
001	1
010	0
011	1
100	0
101	1
110	1
111	0

Combinatorial cube



Binary decision diagram



34

# Introduction

- Different Boolean-function representations have their own strengths and weaknesses
  - They affect the computational efficiency of Boolean manipulations in logic synthesis, hardware/software verification, and many other applications
- Truth tables, Boolean expressions, and logic circuits will be our main use in representing Boolean functions
  - **Boolean expressions** and **logic circuits** are closely related
    - They are built up from *logic operators* and *Boolean variables*


35

# Basic Operations

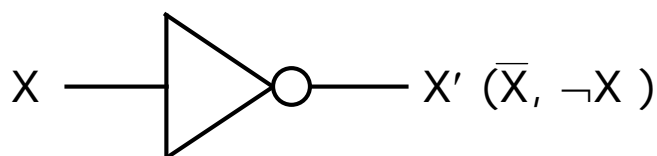
- Three most basic operations in Boolean algebra: {AND, OR, NOT}
  - They form a **functionally complete** set of operations, that is, any Boolean functions can be constructed using these three operations (why?)
  - Are {AND, NOT} functionally complete?

36

# Basic Operations NOT

- NOT (complement, or inverse)
  - Notation: “ ' ”, “-”, or “¬”
  - Logic gate symbol: 

$$\begin{cases} 0' = 1 \\ 1' = 0 \end{cases} \quad \begin{cases} X' = 1 \text{ if and only if } X = 0 \\ X' = 0 \text{ if and only if } X = 1 \end{cases}$$



X	X'
0	1
1	0

NOT-gate, inverter

37

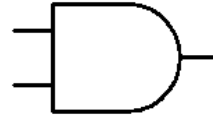
# Basic Operations

## AND

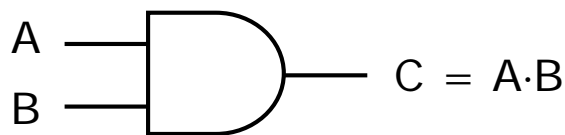
### AND (conjunction)

■ Notation: “ $\cdot$ ”, “ $\wedge$ ”

■ Logic gate symbol:



$$\begin{cases} 0 \cdot 0 = 0 \\ 0 \cdot 1 = 0 \\ 1 \cdot 0 = 0 \\ 1 \cdot 1 = 1 \end{cases}$$



AND-gate

AB	$C = A \cdot B$
00	0
01	0
10	0
11	1

38

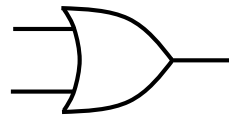
# Basic Operations

## OR

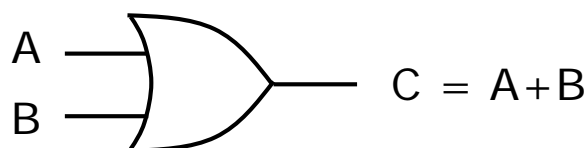
### OR (disjunction)

■ Notation: “ $+$ ”, “ $\vee$ ”

■ Logic gate symbol:



$$\begin{cases} 0 + 0 = 0 \\ 0 + 1 = 1 \\ 1 + 0 = 1 \\ 1 + 1 = 1 \end{cases}$$



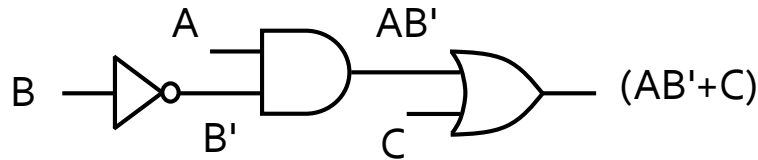
OR-gate

AB	$C = A + B$
00	0
01	1
10	1
11	1

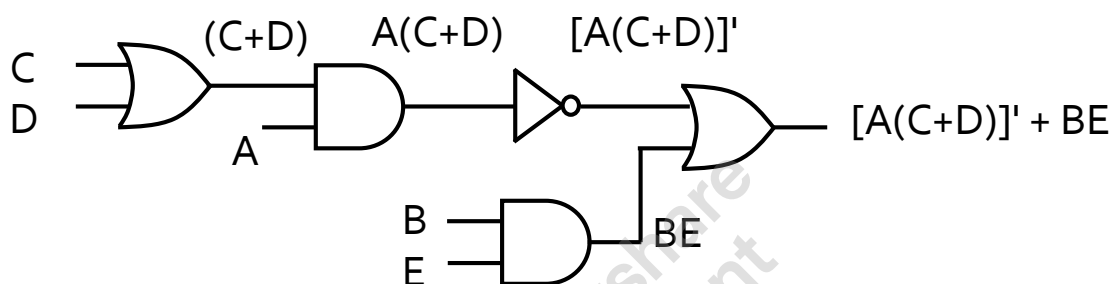
39

## Boolean Expressions & Logic Circuits

### □ $AB' + C$



### □ $[A(C+D)]' + BE$



39

## Boolean Expressions & Logic Circuits

- Given a Boolean expression, we can construct a functionally equivalent logic circuit (not unique)
- Given a logic circuit, we can derive a Boolean expression of the corresponding Boolean function
- Given a Boolean expression or logic circuit, we can derive the truth table of the corresponding Boolean function

40

## Boolean Expressions & Logic Circuits

- A Boolean expression (logic circuit) gives a unique Boolean function
  - The converse is not true, that is, a Boolean function can be represented by different Boolean expressions (logic circuits)
  
- A truth table gives a unique Boolean function, and vice versa
  - Truth tables are **canonical** in representing Boolean functions
  - Can use truth tables to show the equivalence of two Boolean functions

41

## Boolean Expressions & Truth Tables

Truth-table proof of  $AB' + C = (A + C)(B' + C)$   
(equivalence under all truth assignments)

ABC	B'	AB'	$AB' + C$	A+C	B'+C	$(A+C)(B'+C)$
000	1	0	0	0	1	0
001	1	0	1	1	1	1
010	0	0	0	0	0	0
011	0	0	1	1	1	1
100	1	1	1	1	1	1
101	1	1	1	1	1	1
110	0	0	0	1	0	0
111	0	0	1	1	1	1

42

# Basic Theorems of Boolean Algebra

## □ Operations with 0 and 1:

$$\blacksquare X + 0 = X \overset{\text{dual}}{\iff} X \cdot 1 = X$$

$$\blacksquare X + 1 = 1 \iff X \cdot 0 = 0$$

## □ Idempotent laws

$$\blacksquare X + X = X \iff X \cdot X = X$$

Duality: interchange "0" and "1" and interchange "+" and "."

43

# Basic Theorems of Boolean Algebra

## □ Involution law

$$\blacksquare (X')' = X$$

## □ Laws of complementarity

$$\blacksquare X + X' = 1 \iff X \cdot X' = 0$$

Applications to logic simplification

$$\text{E.g., } (AB' + D)E + 1 = 1$$

$$(AB' + D)(AB' + D)' = 0$$

44

# Boolean Algebra with Switches

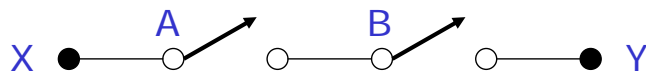


X and Y are connected if and only if  $S = 1$

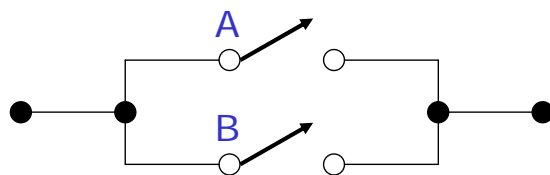
The connectivity between X and Y is a function over S

45

# Boolean Algebra with Switches



X and Y are connected if and only if  $A \cdot B = 1$



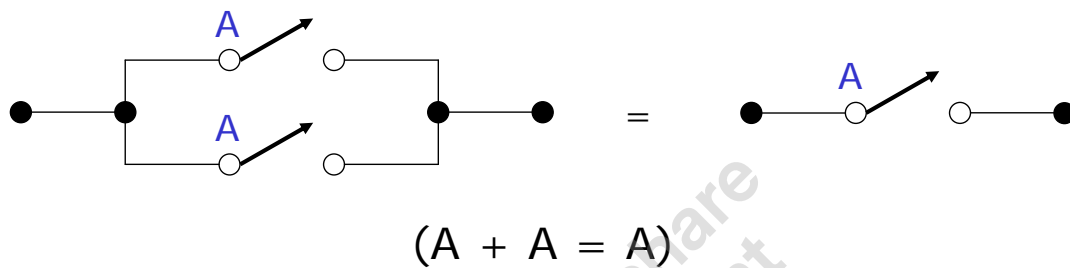
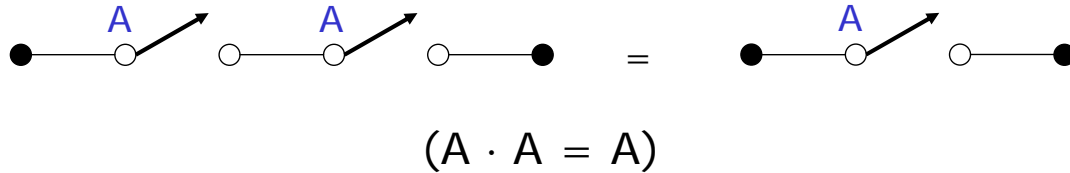
X and Y are connected if and only if  $A + B = 1$

46

# Boolean Algebra with Switches

## Basic Theorems Revisited

### □ Idempotent laws

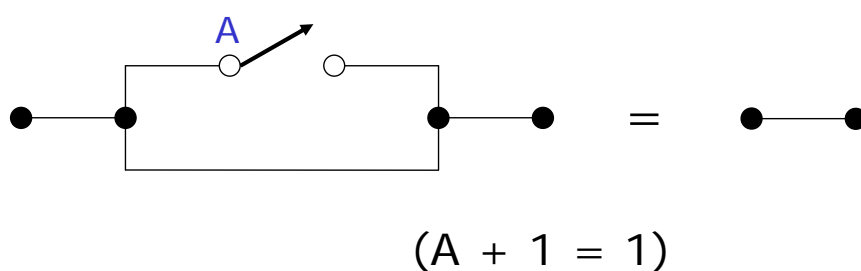
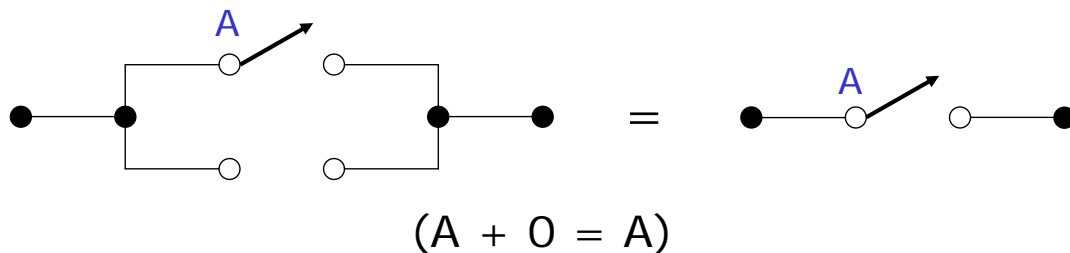


47

# Boolean Algebra with Switches

## Basic Theorems Revisited

### □ Operations with 0 and 1



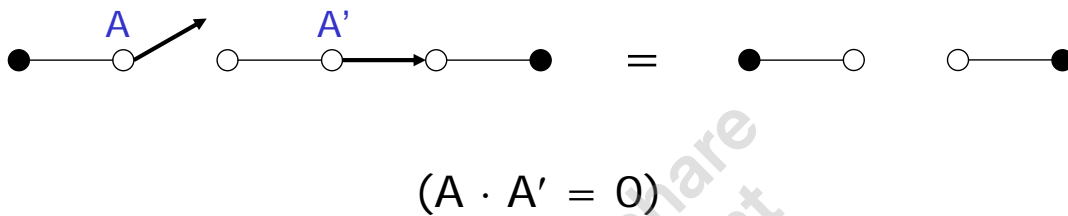
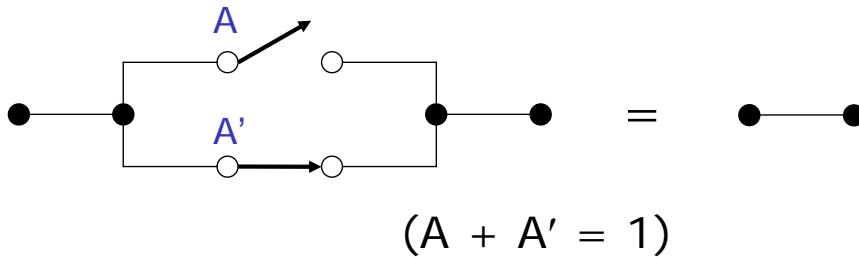
48



# Boolean Algebra with Switches

## Basic Theorems Revisited

### □ Laws of complementarity

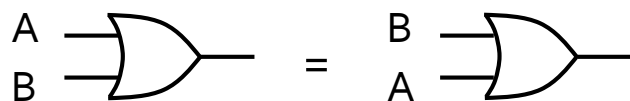
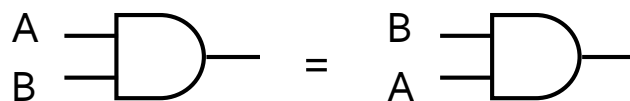


49

## Commutative, Associative, and Distributive laws

### □ Commutative laws

$$\blacksquare X \cdot Y = Y \cdot X \iff X + Y = Y + X$$



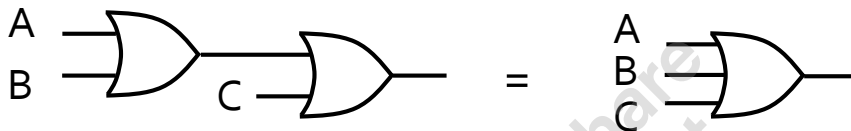
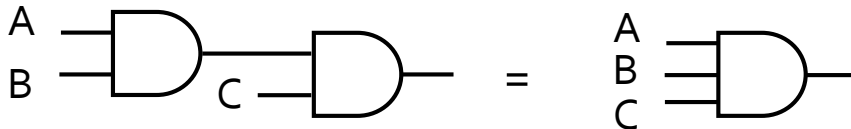
50

# Commutative, Associative, and Distributive laws

## □ Associative laws

$$\blacksquare (XY)Z = X(YZ) = XYZ \iff$$

$$(X+Y)+Z = X+(Y+Z) = X+Y+Z$$



51

# Commutative, Associative, and Distributive laws

## □ Distributive laws

$$\blacksquare X(Y+Z) = XY+XZ \iff X+YZ = (X+Y)(X+Z)$$

- The second equality is valid for Boolean algebra but not for ordinary algebra

Proof.

$$(X+Y)(X+Z) =$$

$$XX+XZ+YX+YZ =$$

$$X+XZ+XY+YZ =$$

$$X \cdot 1 + XZ + XY + YZ =$$

$$X(1+Z+Y) + YZ =$$

$$X \cdot 1 + YZ =$$

$$X+YZ$$

52

## Simplification Theorems

$$\square XY + XY' = X \iff (X+Y)(X+Y') = X$$

$$\square X+XY = X \iff X(X+Y) = X$$

Proof.

$$X+XY = X \cdot 1 + XY = X(1+Y) = X \cdot 1 = X$$

$$X(X+Y) = XX+XY = X+XY = X$$

$$\square (X+Y')Y = XY \iff XY'+Y = X+Y$$

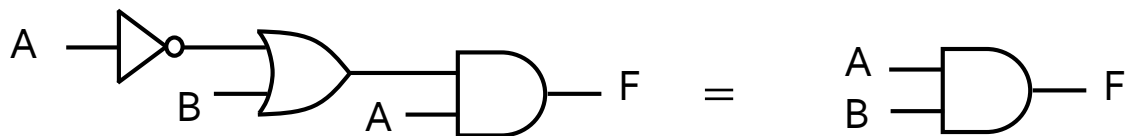
Proof.

$$Y+XY' = (Y+X)(Y+Y') = (Y+X) \cdot 1 = X+Y$$

53

## Logic Circuit Simplification

$$\square F = A(A'+B) = AA'+AB = 0+AB = AB$$



Exercise (p.48)

$$\blacksquare \text{ Simplify } Z = [A+B'C+D+EF] [A+B'C+(D+EF)']$$

$$\blacksquare \text{ Simplify } Z = (AB+C)(B'D+C'E')+(AB+C)'$$

54

# Multiplying Out and Factoring

- Sum-of-products (SOP), or Disjunctive Normal Form (DNF)
  - Sum of products of **literals** (a literal is a variable  $x$  or its complement  $x'$ )
    - E.g.,  $ab'c+a'bd$       yes
    - $a+b+c$               yes
    - $abc$                     yes
    - $a(b'+c)+a'bd$       no
  - Any Boolean function can be represented in the SOP form  
(Why?)
  
- Product-of-sums (POS), or Conjunctive Normal Form (CNF)
  - Product of **clauses** (a clause is a sum of literals)
    - E.g.,  $(a+b+c)(a'+d)$     yes
    - $(a+b+c)$               yes
    - $(a)(b)(c)$             yes
    - $(a+bc)(a'+d)$       no
  - Any Boolean function can be represented in the POS form  
(Why?)

55

# Multiplying Out

- SOP
  - When multiplying out an expression (to obtain an SOP), the 2nd distributive law  
 $(X+Y)(X+Z) = X+YZ$   
 can be applied first when possible to simply the expression

E.g.,

$$\underline{(A+BC)}\underline{(A+D+E)} = \underline{A+BC}\underline{(D+E)} = A+BCD+BCE$$

$$X \quad Y \quad X \quad Z \quad X \quad Y \quad Z$$

In contrast to,

$$\begin{aligned} (A+BC)(A+D+E) &= A+AD+AE+ABC+BCD+BCE \\ &= A(1+D+E+BC)+BCD+BCE = A+BCD+BCE \end{aligned}$$

56

# Factoring

## □ POS

- Apply distributive laws

$$XY + XZ = X(Y + Z)$$

$$X + YZ = (X + Y)(X + Z)$$

to factor an expression in the POS form

- Any expression can be factored to the POS form
- An expression cannot be further factored if and only if it is in the POS form

E.g.,

$$(A + B'CD) = (A + B')(A + CD) = (A + B')(A + C)(A + D)$$

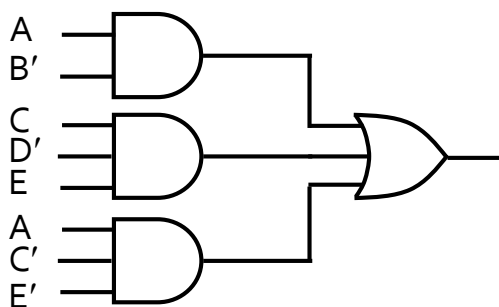
$$(AB' + CD) = (AB' + C)(AB' + D) = (A + C)(B' + C)(A + D)(B' + D)$$

Exercise (p.51): Factor  $(C'D + C'E' + G'H)$

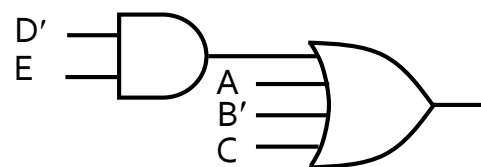
57

# Multiplying Out and Factoring

## □ SOP in AND-OR circuit



$$AB' + CD'E + AC'E'$$

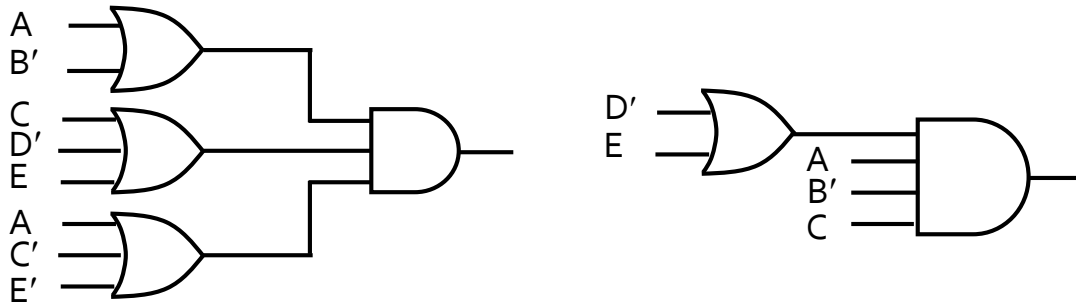


$$A + B' + C + D'E$$

58

# Multiplying Out and Factoring

## □ POS in OR-AND circuit



$$(A+B')(C+D'+E)(A+C'+E')$$

$$AB'C(D'+E)$$

59

# DeMorgan's Laws

## □ Complement by DeMorgan's laws

- $(X+Y)' = X' \cdot Y'$
- $(X \cdot Y)' = X' + Y'$

Proof by truth table

XY	X+Y	$(X+Y)'$	$X' \cdot Y'$	XY	$(X \cdot Y)'$	$X' + Y'$
00	0	1	1	0	1	1
01	1	0	0	0	1	1
10	1	0	0	0	1	1
11	1	0	0	1	0	0

60

# Generalized DeMorgan's Laws

- $(X_1 + X_2 + \dots + X_n)' = X_1' X_2' \dots X_n'$ 
  - Complement of sum = product of complements
- $(X_1 X_2 \dots X_n)' = X_1' + X_2' + \dots + X_n'$ 
  - Complement of product = sum of complements

E.g.,

$$[(A'+B)C']' = (A'+B)' + (C')' = AB' + C$$

$$[(AB'+C)D'+E]' = [(AB'+C)D']'E' = [(AB'+C)'+D]E' = [(AB')'C'+D]E' = [(A'+B)C'+D]E'$$

81

# Duality

- The dual  $F^D$  of an expression  $F$  is formed by replacing AND with OR, OR with AND, 0 with 1, and 1 with 0
  - $F^D$  can also be obtained by complementing  $F$  and then complementing each individual variable

E.g.,

$$(AB'+C)^D = (A+B')C$$

- Equalities are preserved under duality, i.e.,  $F = G$  iff  $F^D = G^D$  (justify prior theorems)

E.g.,

$$X(Y+Z) = XY+XZ \quad \longleftrightarrow \quad \text{dual} \quad X+YZ = (X+Y)(X+Z)$$

62

## UNIT 3

# Applications of Boolean Algebra: Claude Shannon and Circuit Design

## 1 Introduction

On virtually the same day in 1847, two major new works on logic were published by prominent British mathematicians: *Formal Logic* by Augustus De Morgan (1806–1871) and *The Mathematical Analysis of Logic* by George Boole (1815–1864). Both authors sought to stretch the boundaries of traditional logic by developing a general method for representing and manipulating logically valid inferences or, as De Morgan explained in an 1847 letter to Boole, to develop ‘mechanical modes of making transitions, with a notation which represents our head work’ [18, p. 25]. In contrast to De Morgan, however, Boole took the significant step of explicitly adopting *algebraic* methods for this purpose. As De Morgan himself later proclaimed, “Mr. Boole’s generalization of the forms of logic is by far the boldest and most original . . .” (as quoted in [13, p. 174]).

Boole further developed his bold and original approach to logic in his 1854 publication *An Investigation of the Laws of Thought*<sup>1</sup>. In this work, Boole developed a system of symbols ( $\times$ ,  $+$ ) representing operations on classes (or sets) which were symbolically represented by letters. In essence, his logical multiplication  $xy$  corresponded to today’s operation of set intersection, and his logical addition  $x + y$  to today’s operation of set union.<sup>2</sup> Using these definitions, Boole then developed the laws of this ‘Algebra of Logic,’ many of which also held true in ‘standard algebra’. Other laws, however, differed substantially from those of standard algebra, such as the *Idempotent Law*<sup>3</sup>:  $x^2 = x$ .

As noted by Boole, the Idempotent Law holds in standard algebra only when  $x = 0$  or  $x = 1$ . He further commented [4, p. 47] that for

... an Algebra in which the symbols  $x$ ,  $y$ ,  $z$ , &c. admit indifferently of the values 0 and 1, and of these values alone . . . the laws, the axioms, and the processes . . . will be identical in their whole extent with the laws, the axioms, and the processes of an Algebra of Logic.

---

\*Department of Mathematics and Physics; Colorado State University-Pueblo; Pueblo, CO 81001 - 4901; [janet.barnett@colostate-pueblo.edu](mailto:janet.barnett@colostate-pueblo.edu).

<sup>1</sup>For further details on Boole’s work in logic and modifications made to it by John Venn (1834–1923) and C. S. Peirce (1839–1914), see the project “Origins of Boolean Algebra in the Logic of Classes: George Boole, John Venn and C. S. Peirce,” Janet Barnett author.

<sup>2</sup>For various technical reasons, Boole restricted his use of  $+$  to classes which were disjoint. Most of his immediate followers, however, relaxed this restriction, so that their use of  $+$  corresponded exactly to today’s operation of set union. British mathematician John Venn (1834–1923) discussed this issue in detail in the second (1894) edition of his *Symbolic Logic* [20, pp. 42-46]. Ultimately, Venn adopted an unrestricted use of  $+$  ‘partly . . . because the voting has gone this way, and in a matter of procedure there are reasons for not standing out against such a verdict . . .’.

<sup>3</sup>For Boole, the Idempotent Law followed directly from the definition of  $xy$  as ‘the whole of that class of objects to which the names or qualities represented by  $x$  and  $y$  are together applicable’, from which ‘it follows that if the two symbols have exactly the same signification, their combination expresses no more than either of the symbols taken alone would do.’ (See [4, p. 31].) Selecting the sheep from the class of sheep, for instance, gives us just the class of sheep, so that  $xx = x$ .



In the early twentieth century, this special two-valued ‘arithmetical algebra’ became important in the axiomatization of boolean algebras; Edward V. Huntington, for example, employed it as a model for one of three postulate sets for boolean algebra in his 1904 paper *Sets of Independent Postulates for the Algebra of Logic*<sup>4</sup>. In that work, Huntington defined addition and multiplication (which he denoted by  $\oplus$  and  $\odot$  respectively) by the following tables [10, p. 293]:

$$\begin{array}{c|cc} \oplus & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad \begin{array}{c|cc} \odot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

For Huntington, these tables defined a completely abstract (i.e., meaningless) system. For Boole, the equalities represented in these tables (e.g.,  $1 + 1 = 1$ )<sup>5</sup> would have represented statements about sets (i.e., the union of the universal set with itself is again the universal set). In this project, we will see how this same two-valued system was employed in another concrete application of boolean algebra in the mid-twentieth century: the design and analysis of circuits.

## 2 Claude Shannon, Boolean Algebra and Circuit Design

The algebraic methods introduced by Boole for the study of logic attracted considerable attention from mathematicians in the years following publication of *Laws of Thought*. Alongside various refinements and extensions made to Boole’s system during this time, mathematics itself underwent significant changes, becoming both increasingly abstract and more formal in its approach to proof. In line with this trend came a loosening of the ties between the algebraic system introduced by Boole and logic as a concrete interpretation of that system. In his classic *The Algebra of Logic* of 1914, for example, French mathematician Louis Couturat (1868–1914) went so far as to declare [6, p. 1]:

The formal value of this calculus and its interest for the mathematician are absolutely independent of the interpretation given it and of the application which can be made of it to logical problem. In short, we shall discuss it not as logic but as algebra.<sup>6</sup>

It was not long, however, before individuals interested in problems outside of mathematics proper gained exposure to boolean algebra and its unique properties, thanks in part to the work of Couturat

<sup>4</sup>For further details on Huntington’s work, see the project “Boolean Algebra as an Abstract Structure: Edward V. Huntington and Axiomatization,” Janet Barnett author.

<sup>5</sup>In Boole’s ‘Algebra of Logic’, the symbols ‘0’ and ‘1’ denoted two special classes: ‘nothing’ (‘empty set’) and ‘universe’ (‘universal set’) respectively. To justify the use of these symbols, Boole used the analogy between the roles played by these numbers in algebra and the roles played by these special classes in logic [4, p. 47–48]. He argued, for example, that since  $0y = 0$  in standard algebra, then ‘...we must assign to the symbol 0 such an interpretation that the class represented by  $0y$  may be identical with the class represented by 0, whatever the class  $y$  may be. A little consideration will show that this condition is satisfied if the symbol 0 represent Nothing.’ A similar analysis of the algebraic equation  $1y = y$  led him to conclude that ‘...the class represented by 1 must be “the Universe,” since this is the only class in which are found all the individuals that exist in any class.’

<sup>6</sup>Similarly, Huntington opened his 1904 paper with the following declaration [10, p. 288]: “The algebra of symbolic logic, as developed by LEIBNIZ, BOOLE, C.S. PEIRCE, E. SCHRÖDER, and others is described by WHITEHEAD as *the only known member of the non-numerical genus of universal algebra*. This algebra, although originally studied merely as a means of handling certain problems in the logic of classes and the logic of propositions, has recently assumed some importance as an independent calculus; it may therefore be not without interest to consider it from a purely mathematical or abstract point of view, and to show how the whole algebra, in its abstract form, may be developed from a selected set of fundamental propositions, or postulates, which shall be independent of each other, and from which all the other propositions of the algebra can be deduced by purely formal processes. In other words, we are to consider the construction of a purely *deductive theory*, without regard to its possible applications.”

and other mathematicians interested solely in its formal algebraic structure. A 1949 list of some of the applications which resulted from that exposure — applications largely undreamed of by Boole and his Victorian colleagues — included “an axiomatic formulation of biology, the study of neural networks in the nervous systems, the analysis of insurance policies, probability and set theory, etc. [16, p. 588]”. The compiler of this list, American mathematician and electrical engineer Claude E. Shannon (1916–2001), himself gained reknown for a particular application of boolean algebra.

Shannon completed bachelor degrees in both mathematics and electrical engineering at the University of Michigan in 1936. Two years later, at the age of 22, he completed a master’s thesis in electrical engineering at the Massachusetts Institute of Technology. The idea which inspired his thesis work came from his exposure to symbolic logic in an undergraduate philosophy course. Vannevar Bush (1890–1974), dean of engineering at MIT and inventor an early mechanical computer called the differential analyser machine, was sufficiently impressed by Shannon’s thesis to sponsor its publication in an engineering journal. This award-winning paper went on to revolutionize the study of switches and relays, which in turn form the circuitry behind the binary arithmetic of modern computers.<sup>7</sup> Shannon then completed a doctorate in mathematics at MIT with a thesis on the application of mathematics to genetics, and began his official career as a research mathematician at Bell Laboratories in 1941. His association with Bell Labs, either as full time scientist or as a consultant, continued until 1971. In 1948, he published yet another ground breaking paper, *A Mathematical Theory of Communication*, thereby launching the still flourishing field of information theory. He married in 1949 (he and his wife had four children), and served as a faculty member and researcher at MIT from 1956 through 1978. His work included important contributions to cryptography, game theory and computer science; Shannon is also remembered for various mechanical inventions, and for his successful stock investment strategies. Among his many honors was the first ever Marconi Lifetime Achievement Award, awarded to him in 2000. By this time, sadly, Shannon suffered significantly from the effects of Alzheimer’s disease; he died in a nursing home just a year later.

In the 1938 paper based on his master’s thesis, *A Symbolic Analysis of Relay and Switching Circuits*, Shannon described the general problem to be solved and his proposed approach to it as follows [14, p. 713]:

○○○○○○○○○○

In the control and protective circuits of complex electrical systems it is frequently necessary to make intricate interconnections of relay contacts and switches. Examples of these circuits occur in automatic telephone exchanges, industrial motor-control equipment, and in almost any circuits designed to perform complex operations automatically. In this paper a mathematical analysis of certain of the properties of such networks will be made. . . .

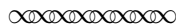
The method of attack on these problems may be described briefly as follows: any circuit is represented by a set of equations, the terms of the equations corresponding to the various relays and switches in the circuit. A calculus is developed for manipulating these equations by simple mathematical processes, most of which are similar to ordinary algebraic algorisms. This calculus is shown to be exactly analogous to the calculus of propositions used in the symbolic study of logic.

○○○○○○○○○○

On one level, the key to applying symbolic boolean algebra to relay and switching circuits lay in the fact that there are only two possible states for such circuits, open and closed, a situation reminiscent of Boole’s special algebra on two symbols, 0 and 1. In fact, the arithmetical version of

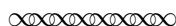
<sup>7</sup>For more information on the connection of switch/relay circuitry to binary arithmetic, see the project “Arithmetic Backwards from Shannon to the Chinese Abacus,” Jerry Lodder author.

Shannon's postulates for networks as stated in this paper [14, p. 713] is identical to Huntington's two-valued model of boolean algebra (see page 2 of this project):

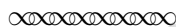


### Postulates

1. *a.*  $0 \cdot 0 = 0$   
*b.*  $1 + 1 = 1$
2. *a.*  $1 + 0 = 0 + 1 = 1$   
*b.*  $0 \cdot 1 = 1 \cdot 0 = 0$
3. *a.*  $0 + 0 = 0$   
*b.*  $1 \cdot 1 = 1$
4. At any given time either  $X = 0$  or  $X = 1$ .



In a 1987 interview<sup>8</sup> with *Omni* magazine, Shannon elaborated on the basic underlying analogy between circuits and boolean algebra in response to the question 'Was the basic insight that yes/no can be embodied in on/off switches so trivial?' with the following comments [17, p. xxvi]:



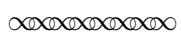
It's not so much that a thing is "open" or "closed," the "yes" or "no" that you mentioned. The real point is that two things in series are described by the word "and" in logic, so you would say this "and" this, while two things in parallel are described by the word "or." The word "not" connects with the back contact of a relay rather than the front contact. There are contacts which close when you operate the relay, and there are other contacts which open, so the word "not" is related to that aspect of relays. All of these things together form a more complex connection between Boolean algebra, if you like, or symbolic logic, and relay circuits.

The people who had worked with relay circuits were, of course, aware of how to make these things. But they didn't have the mathematical apparatus of the Boolean algebra to work with them, and to do them efficiently. . . .

They all knew the simple fact that if you had two contacts in series both had to be closed to make a connection through. Or if they are in parallel, if either one is closed the connection is made. They knew it in that sense, but they didn't write down equations with plus and times, where plus is like a parallel connection and times is like a series connection.<sup>9</sup>

<sup>8</sup>In this same interview [17, pp. xxv-xxvi], Shannon described the act of making the connection between Boolean algebra and a relay circuit as "not the main thing" and declared that "[t]he more important, harder part was working out the details, how to interleave the topology of the switching circuits, the way the contacts are connected up and so on, with the Boolean algebra expressions. Working that out was a lot of fun. I think I had more fun doing that than anything else in my life, creatively speaking. "

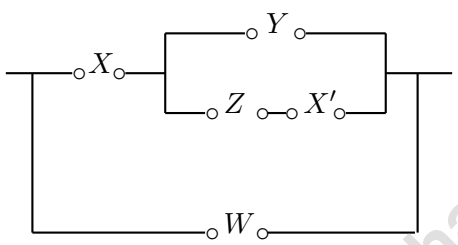
<sup>9</sup>In the only two scholarly articles which he published on this subject [14, 16], Shannon focused on 'hindrance' or 'impedance' at a contact as the central physical characteristic, rather than 'flow' across the contact resulting from a connection being made. Under the impedance interpretation, an open circuit is said to have *infinite impedance* and a closed circuit is said to have *zero impedance*; in this interpretation, 'plus' corresponds to a series connection (infinite impedance when either the first *or* the second contact have infinite impedance:  $a + b = 1$  iff  $a = 1$  or  $b = 1$ ), while 'times' corresponds to a parallel connection (infinite impedance when the first *and* the second contact have infinite impedance:  $a \cdot b = 1$  iff  $a = 1$  and  $b = 1$ ). Owing to the dual principle of Boolean algebra, either interpretation (hindrance or flow) can be used with equal ease. In the interest of consistency with current textbook writing, we deviate from Shannon's original interpretation and base all exercises in this project on the 'flow' interpretation as described in Shannon's 1987 interview above; examples from Shannon's earlier papers are modified accordingly.



In other words, the application of Boolean algebra to circuits provided an actual physical representation for the corresponding symbolic operations. Diagrams depicting the two types of connections and the corresponding operations are shown in Figure 1 below. An example of how to represent a more complicated circuit with an algebraic equation, based on an example from Shannon [16, p. 589], is shown in Figure 2.



Figure 1



Network for boolean expression  $W + X \cdot (Y + Z \cdot X')$

1. Shannon employed the notation  $X'$  to represent the 'negative of  $X$ ', or 'not- $X$ '; thus, the contact  $X'$  is closed (connection made between terminal points) whenever the contact  $X$  is open (no connection made between terminal points), and vice versa. Explain why the overall network in Figure 2 is closed when contact  $W$  is closed, regardless of the states of contacts  $X$ ,  $Y$  and  $Z$ . Then determine whether this network is open or closed when contact  $W$  is open and contacts  $X$ ,  $Y$  and  $Z$  are closed; explain your conclusion.
2. Represent the network in Figure 3 (adapted from [14, p. 715]) by a Boolean expression, using  $+$  for parallel connections and  $\cdot$  series for connections.

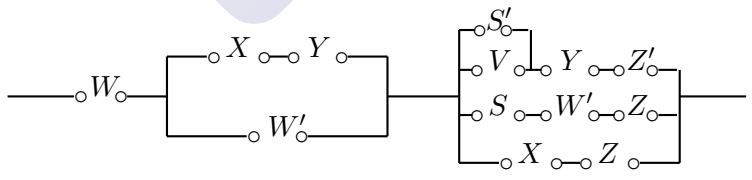


Figure 3: Network for project question 2.

3. Sketch the network represented by the Boolean expression  $X + Y(Z + W) + X'Z$ , again using  $+$  for parallel connections and  $\cdot$  series for connections.

Shannon used diagrams such as these not only to represent given circuits, but also to illustrate Boolean algebra identities. The following excerpt gives his description of the basic Boolean identities for circuits [14, p. 713-714].



$$X + Y = Y + X \quad (1a)$$

$$XY = YX \quad (1b)$$

$$X + (Y + Z) = (X + Y) + Z \quad (2a)$$

$$X(YZ) = (XY)Z \quad (2b)$$

$$X(Y + Z) = XY + XZ \quad (3a)$$

$$X + YZ = (X + Y)(X + Z) \quad (3b)$$

$$1 \cdot X = X \quad (4a)$$

$$0 + X = X \quad (4b)$$

$$1 + X = 1 \quad (5a)$$

$$0 \cdot X = 0 \quad (5b)$$

...

Due to the associative laws (2a and 2b) parentheses may be omitted in a sum or product of several terms without ambiguity. ...

The distributive law (3a) makes it possible to "multiply out" products and to factor sums. The dual of this theorem (3b), however, is not true in numerical algebra.

... The negative of a hindrance  $X$  will be written  $X'$  and is defined as a variable which is equal to 1 when  $X$  equals 0 and equal to 0 when  $X$  equals 1. ... The definition of the negative of a hindrance gives the following theorems:

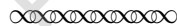
$$X + X' = 1 \quad (6a)$$

$$XX' = 0 \quad (6b)$$

$$0' = 1 \quad (7a)$$

$$1' = 0 \quad (7b)$$

$$(X')' = X \quad (8)$$



Many of the laws listed above by Shannon are familiar from standard algebra. The most unfamiliar law, perhaps, is his (3b):  $X + YZ = (X + Y)(X + Z)$ . The fact that (logical) addition is distributive over (logical) multiplication was, however, already a familiar boolean algebra property to Shannon's predecessors. The following question examines this law from the perspective of circuits.

4. Figure 4 below (adapted from [16, p. 591]) uses network diagrams to illustrate the distributive law (3b). Explain why these two circuits are equivalent by discussing what configurations of open (no connection made) and closed (connection is made) contacts are needed for flow across the overall network.

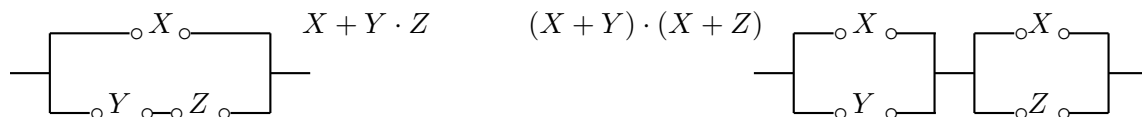


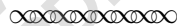
Figure 4: Network for project question 4.

Now complete the table on the following page to show that the two Boolean expression are equivalent for all possible values of the variables in the boolean algebra on  $\{0, 1\}$ .

$X$	$Y$	$Z$	$YZ$	$X + Y$	$X + Z$	$X + YZ$	$(X + Y)(X + Z)$
0	0	0					
0	0	1					
0	1	0					
0	1	1					
1	0	0					
1	0	1					
1	1	0					
1	1	1					

Shannon referred to the proof technique in which all possible cases are directly verified, as is done in the above table, as the ‘method of perfect induction’ [14, p. 714]. In light of its simplicity, his 1938 paper included only one proof as an illustration of the technique. As Shannon himself noted, however, this proof technique is helpful in the context of circuits precisely because ‘each variable is limited to just two values’ [14, p. 714]. Since this is not the case for all boolean algebras, establishing these identities in general required more sophisticated proof techniques, such as those used in Huntington’s 1904 paper on the axiomatization of boolean algebra. Because Shannon was interested in applying the properties of general boolean algebras to the specific two-valued boolean algebra defined by circuits, he proceeded to show that the two-valued algebra of circuits did, in fact, satisfy all Huntington’s axioms for a general boolean algebra. As a consequence, any property which could be proven for a general boolean algebra necessarily held for the specific two-valued algebra of circuits.

Having established this correspondence, Shannon next listed several other boolean algebra identities, citing them as immediate consequences of the equivalence between circuits and symbolic logic. Among the more important of these were the following [14, pp. 714–715]:



$$(X + Y + Z + \dots)' = X' \cdot Y' \cdot Z' \dots \quad (9a)$$

$$(X \cdot Y \cdot Z \dots)' = X' + Y' + Z' \dots \quad (9b)$$

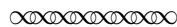
.....

$$X = X + X = X + X + X = \text{etc.} \quad (14a)$$

$$X = X \cdot X = X \cdot X \cdot X = \text{etc.} \quad (14b)$$

$$X + XY = X \quad (15a)$$

$$X(X + Y) = X \quad (15b)$$



Notice that, as he had already done with the first three postulates for circuits and with the basic identities (1) - (7), Shannon arranged these additional properties as pairs ‘to emphasize a duality relationship between the operations of addition and multiplication and the quantities zero and one’ [14, pp. 713]. Examine these various dual pairs carefully before responding to the following question.

5. Carefully examine Shannon's dual pairs of properties (1) - (7), (9), (14) and (15).
- Write a short description of how to obtain the dual of a statement.
  - Illustrate your method by writing the dual of the following expressions. For each, represent both the original expression and its dual by a network.
    - $X + YZ$
    - $(X + Y)(Z + W)$
    - $XZ' + Y + W'$
  - Consider the network you sketched in part (b) for the expression (i), and determine the configurations of open (no connection made) and closed (connection is made) contacts that are needed for flow across the overall network. Then do the same for the network which represents the dual of expression (i). Comment on how these two sets of configurations (for the original and for its dual) compare.

This principle of duality was also well-known to Shannon's predecessors, and served as 'a characteristic feature of the algebra' [10, p. 294]. As noted by Shannon, this principle also 'gives each theorem a dual theorem, it being necessary to prove only one to establish the both.' [14, pp. 713]. Thus, as an immediate consequence of the Idempotent Law for Multiplication — Boole's  $x^2 = x$  and Shannon's Property (14b) — we are able to conclude that the Idempotent Law for Addition — Shannon's Property (14a) — is also valid. The following question explores the use of Shannon's method of perfect induction and the principle of duality within the context of Shannon's Identities (9ab) and (15ab), known as DeMorgan's Laws and Absorption respectively.

6. This question examines the Laws of Absorption, Shannon's Properties (15ab), in more detail.
- First complete the following table for the first of two Absorption Laws, and comment on how it proves the validity of this property within the context of circuits.

$X$	$Y$	$XY$	$X + XY$
0	0		
0	1		
1	0		
1	1		

- Now complete the following table for the second of two Absorption Laws. Compare this to the table in part (a), and comment on how these two tables illustrate the 'duality relationship between the operations of addition and multiplication and the quantities zero and one'.

$X$	$Y$	$X + Y$	$X(X + Y)$
1	1		
1	0		
0	1		
0	0		

- Recall that in Boole's logic of classes, multiplication corresponds to the operation of set intersection and addition corresponds to the operation of set union. Use this interpretation to explain why the Absorption Laws are also valid within this interpretation.

7. This question examines DeMorgan's Laws [Shannon's Properties (9ab)] in more detail.

- (a) For two variables  $X$  and  $Y$ , the first of DeMorgan's Law is the equality:  $(X + Y)' = X' \cdot Y'$ . Complete the following tables to show that this law holds for circuits by the method of perfect induction.

$X$	$Y$	$X + Y$	$(X + Y)'$	$X'$	$Y'$	$X' \cdot Y'$
0	0					
0	1					
1	0					
1	1					

Then use the principle of duality to explain why the following dual version of DeMorgan's Law for two sets is also valid:  $(X \cdot Y)' = X' + Y'$ .

- (b) As Shannon remarked, DeMorgan's Law can be applied to any number of sets. Shannon also described this generalization as a (mechanical) method by which "the negative of any function may be obtained by replacing each variable by its negative and interchanging the + and  $\cdot$  rules. . . . For example, the negative of  $X + Y \cdot (Z + WX')$  will be  $X'[Y' + Z'(W' + X)]$  [14, p. 715]. "

(Note that Shannon is using the word 'negative' here to mean what is usually referred to as the *complement* in current Boolean Algebra usage.)

Without Shannon's method, negation of complicated expressions requires iterative applications of the basic two-set version of De Morgan's Laws:  $(XY)' = X' + Y'$  and  $(X + Y)' = X'Y'$ . For the example considered by Shannon above, for instance, this iterative method would look as follows:

$$\begin{aligned}
 [X + Y \cdot (Z + WX')] &= X' \cdot \underbrace{[Y \cdot (Z + WX')]}' \\
 &= X' \cdot [Y' + \underbrace{(Z + WX')}'] \\
 &= X' \cdot [Y' + (Z' \cdot \underbrace{(WX')}')'] \\
 &= X' \cdot [Y' + Z' \cdot (W' + X'')] \\
 &= X' \cdot [Y' + Z' \cdot (W' + X)]
 \end{aligned}$$

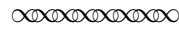
Re-write each of the following by first using Shannon's method, and then via the iterative De Morgan's Law technique. Which method do you prefer, and why?

(i)  $[XY' + Z]'$  (ii)  $[XW(Y' + Z)]'$

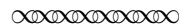
- (c) At one point in his work on general boolean algebras, Huntington showed how De Morgan's Laws can be used to define the operation  $+$  in terms of the operations  $\cdot$  and  $'$ ; namely,  $X + Y = (X' \cdot Y)'$ . Does this mean that all relay networks can be constructed using only seriesconnections? Explain.



One of Shannon's goals in applying boolean algebra to the study of circuits was to use algebraic techniques to simplify complicated systems, as he described in the following excerpt from his 1949 paper *The Synthesis of Two-Terminal Switching Circuits* [16, p. 590].



By means of Boolean Algebra it is possible to find many circuits equivalent in operating characteristics to a given circuit. The hindrance of the given circuit is written down and manipulated according to the rules. Each different resulting expression represents a new circuit equivalent to the given one. In particular, expressions may be manipulated to eliminate elements which are unnecessary, resulting in simple circuits.



For example, the following computation confirms that the element  $Z$  can be eliminated from the network from Figure 2, a fact which careful examination of the network diagram in Figure 2 also reveals:

$$W + X \cdot (Y + Z \cdot X') = W + XY + X(ZX') = W + XY + (XX')Z = W + XY + 0 \cdot Z = W + XY$$

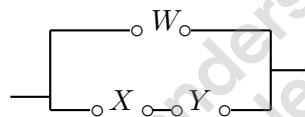


Figure 5: A network equivalent for  $W + X(Y + Z \cdot X')$ .

8. Use boolean algebra identities, including the law of absorption (*Shannon's properties 15ab*) to show that the networks in Figure 6 are equivalent.

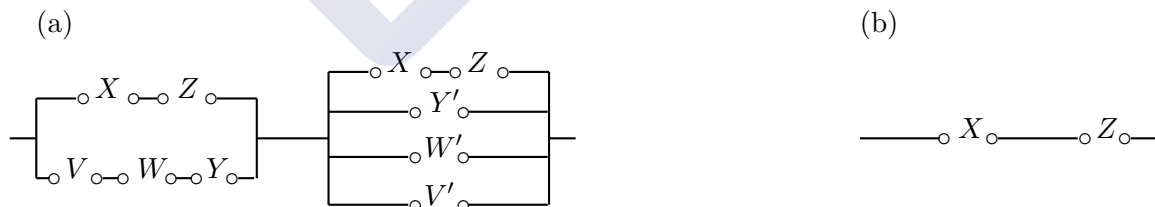


Figure 6: Networks for project question 7.

9. Write a boolean algebra expression for the network in Figure 7:

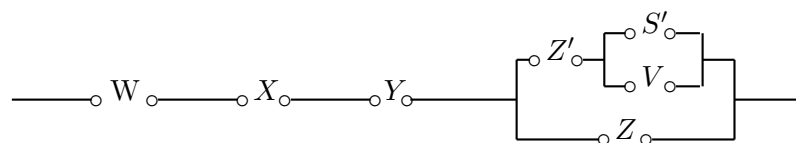


Figure 7: Network for project question 8.

Then use boolean algebra identities to show that the network represented by the following expression is equivalent to the network in Figure 7:

$$W \cdot (XY + W') \cdot [S'YZ' + VYZ' + SWZ + XZ]$$

Finally, sketch the network for the expression  $W \cdot (XY + W') \cdot [S'YZ' + VYZ' + SWZ + XZ]$ , and comment on the relative simplicity of the two equivalent networks.

To algebraically simplify very complicated networks, such as that in Figure 3 above, Shannon employed a method of representing Boolean-valued functions dating back to Boole's own *Laws of Thought* [5]. In fact, this method of representation formed the core of Boole's technique of logical deduction via algebraic manipulation. In the next section, we examine this method of representing Boolean-valued functions in the writings of both Boole and Shannon.

### 3 Boolean Functions and Synthesis of Circuits

In 1892, a supporter of Boole's approach to logic, W. E. Johnson, wrote [11, p. 3]:

As a material machine is an instrument for economising the exertion of force, so a symbolic calculus is an instrument for economising the exertion of intelligence. And, employing the same analogy, the more perfect the calculus, the smaller would be the amount of intelligence applied as compared with the results produced. . . . It will appear that the *logical* calculus stands in a unique relation to intelligence; for it aims at exhibiting, in a non-intelligent form those same intelligent principles that are actually required for working it.

The circuits used in modern computing technology also serve as an economizing instrument for the exertion of both force and intelligence, with Boole's logical calculus providing the necessary non-intelligent, mechanical mode for making them work in required ways. In this closing section of this project, we consider the problem of "synthesis" for circuits: given a specific set of desired inputs and outputs, construct a network of series and parallel connections corresponding to those values.

The mathematical ideas needed to solve this problem were, in fact, developed by Boole in connection with problems in logic. Boole's goal was to take a logical expression that involved any number of logical variables and represent it as a particular kind of sum. For a logical expression  $f(x)$  of just one variable, the desired sum had the form  $f(x) = ax + b(1 - x)$ . Boole referred to this process as "developing  $f(x)$ ". The following excerpt shows how Boole developed a method for computing the coefficients  $a$  and  $b$  in this sum [5, p. 74].

○○○○○○○○○○○○

Assume then,

$$f(x) = ax + b(1 - x),$$

and making  $x = 1$ , we have

$$f(1) = a.$$

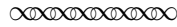
Again, in the same equation making  $x = 0$ , we have

$$f(0) = b.$$

Hence, the values of  $a$  and  $b$  are determined, and substituting them in the first equation, we have

$$f(x) = f(1)x + f(0)(1 - x);$$

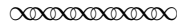
as the development sought<sup>10</sup>.



Using Shannon's notation  $x'$  to denote the expression  $1 - x$ , note that this equation can be re-written as:

$$f(x) = f(1)x + f(0)x'.$$

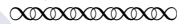
Before looking at a specific example, read Boole's description of how to develop a function  $f(x, y)$  of two variables [5, p. 74]:



... we have

$$f(x, y) = f(1, 1)xy + f(1, 0)x(1 - y) + f(0, 1)(1 - x)y + f(0, 0)(1 - x)(1 - y),$$

for the expansion required. Here  $f(1, 1)$  represents what  $f(x, y)$  becomes when we make therein  $x = 1, y = 1$ ;  $f(1, 0)$  represents what  $f(x, y)$  becomes when we make therein  $x = 1, y = 0$ , and so on for the rest.



10. Using Shannon's notation of  $x'$  for  $1 - x$ , Boole's expansion of  $f(x, y)$  can be written as

$$f(x, y) = f(1, 1)xy + f(1, 0)xy' + f(0, 1)x'y + f(0, 0)x'y'.$$

Use this expansion to verify that the following table of function values defines the function represented by  $f(x, y) = xy + x'y$ .

$x$	$y$	$f(x, y)$
0	0	0
0	1	1
1	0	0
1	1	1

<sup>10</sup>Boole included a footnote at this point in which he showed how to derive this same equation by substituting  $x^n = x$  into the Taylor's series expansion of a function  $f(x)$  and manipulating the result algebraically.

11. Use Boole's notation to write out the eight terms of the expansion for a function of three variables,  $f(x, y, z)$ ; then translate this into Shannon's notation.

Shannon also considered this type of expansion for a function  $f(x_1, x_2, \dots, x_n)$  of  $n$  variables. In both [14, 16], he noted that the expansion will include  $2^n$  terms, where each of these term will have the form ' $Cy_1y_2y_3 \dots y_n$ ' with the coefficient  $C$  equal to either 0 or 1 and each  $y_i$  equal to either  $x_i$  or  $x'_i$ . Today, this form of expansion is referred to as the *disjunctive normal form* of the function.

As an example, note that the function  $f(x, y, z) = x'y + y'z' + xyz$  is NOT in disjunctive normal form as it is written, since the variable  $z$  is missing from the first term, while the variable  $x$  is missing from the second term. However, we can re-write it as  $f(x, y, z) = x'yz + x'y'z' + xy'z' + x'y'z' + xyz$  by noting that  $x'y = x'yz + x'y'z'$  and  $y'z' = xy'z' + x'y'z'$ . (Can you see why these two facts are true?). Although the expression  $f(x, y, z) = x'yz + x'y'z' + xy'z' + x'y'z' + xyz$  contains only 5 non-zero terms, note that it is written in disjunctive normal form since the remaining three terms of the fully expressed disjunctive normal form have zero coefficient, and therefore need not be written out.

The next project question illustrates two methods for finding the disjunctive normal form of any function, given the function as a boolean expression.

12. Consider the function  $f(x, y, z) = yz + xy'$ .
- Calculate the values of  $f(x, y, z)$  for all eight possible values of  $(x, y, z)$ , and use these values in your expansion from project question 11 to find the disjunctive normal form of  $f$ . (You should find four non-zero terms.)
  - Now use the facts that  $x + x' = 1$  and  $z + z' = 1$  to find the disjunctive normal form by expanding  $f(x, y, z) = 1 \cdot (yz) + 1 \cdot (xy')$ .
  - Which method do you prefer, and why?

The remaining project questions in this section illustrate the use of the disjunctive normal form to find a boolean expression of any function, given the function as a table of values.

13. Suppose we wish to build a circuit which corresponds to the following table of values for the function  $f(x, y, z)$ .

$x$	$y$	$z$	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

Use your expansion from project question 11 to find the disjunctive normal form of  $f$ , and simplify your result to show that  $f(x, y, z) = y + xz'$ . Then sketch the network corresponding to  $y + xz'$ . How easy would it have been to determine this circuit directly from the table of values, rather than from its Boolean expression?

14. Find the disjunctive normal form of the function  $f$  represented by the following table; simplify if possible, then use the result to sketch the corresponding network.

$x$	$y$	$z$	$f(x, y, z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

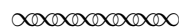
15. Find the disjunctive normal form of the function  $f$  represented by the following table; simplify if possible, then use the result to sketch the corresponding network.

$x$	$y$	$z$	$f(x, y, z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

16. Describe a general method for finding the disjunctive normal form of a Boolean function  $f$  from its table of values.
17. How would you define the *conjunctive normal form* of a Boolean function? Give an example, and discuss possible method(s) for finding this form for a given function in disjunctive normal form and/or from a table of values.

## 4 Boolean Functions and the Simplification of Circuits

We now return to the problem of simplifying complicated circuits using boolean algebra. We begin with an excerpt in which Shannon states the basic theorems he used to simplify boolean functions. Like Boole, Shannon compared this method to a familiar idea from calculus [14, p. 715].



The notation  $f(X_1, X_2, \dots, X_n)$  will be used to represent a function. Thus, we have  $F(X, Y, Z) = XY + X'(Y' + Z')$ . In infinitesimal calculus it is shown that any function (providing it is continuous and all derivatives are continuous) may be expanded in a Taylor series. A somewhat similar expansion is possible in the calculus of propositions. To develop the series expansion of functions first note the following equations.

$$f(X_1, X_2, \dots, X_n) = X_1 \cdot f(1, X_2, \dots, X_n) + X_1' f(0, X_2, \dots, X_n) \quad (10a)$$

$$f(X_1, X_2, \dots, X_n) = [f(0, X_2, \dots, X_n) + X_1] \cdot [f(1, X_2, \dots, X_n) + X_1'] \quad (10b)$$

These reduce to identities if we let  $X_1$  equal either 0 or 1. In these equations the function  $f$  is said to be expanded about  $X_1$ .

Some other theorems useful in simplifying expressions are given below:

...

$$Xf(X, Y, \dots, Z) = Xf(1, Y, \dots, Z) \quad (17a)$$

$$X + f(X, Y, \dots, Z) = X + f(0, Y, \dots, Z) \quad (17b)$$

...

All of these theorems may be proved by the method of perfect induction.

...

○○○○○○○○○○

18. Verify that Shannon's identity 10a using his method of perfect induction.

That is, first show that this identity holds in the case  $X_1 = 0$ , simplifying the right-hand side as needed, and then verify that this identity holds in the case  $X_1 = 1$ .

Then provide a similar proof for Shannon's identity 10b.

19. Verify that Shannon's identity 17a using his method of perfect induction.

Then provide a similar proof for Shannon's identity 17b.

We now illustrate how Shannon used the expansion about one variable given in identity 17b to simplify circuits by considering an example from [14, p. 715] in which Shannon simplifies the circuit represented by the following boolean expression:<sup>11</sup>

$$X_{ab} = W + W'(X + Y) + (X + Z)(S + W' + Z)(Z' + Y + S'V)$$

The following excerpt gives Shannon's simplification with minimal explanation provided; in project question 20, we examine the derivation in more detail.

○○○○○○○○○○

$$\begin{aligned} X_{ab} &= W + W'(X + Y) + (X + Z)(S + W' + Z)(Z' + Y + S'V) \\ &= W + X + Y + (X + Z)(S + 1 + Z)(Z' + Y + S'V) \\ &= W + X + Y + Z \cdot (Z' + Y + S'V) \end{aligned}$$

These reductions were made with 17b using first  $W$ , then  $X$  and  $Y$  as the "X" of 17b. Now multiplying out

$$\begin{aligned} X_{ab} &= W + X + Y + ZZ' + ZY + ZS'V \\ &= W + X + Y + ZS'V \end{aligned}$$

○○○○○○○○○○

<sup>11</sup>Note that this expression is the dual of the expression for the circuit shown in Figure 3 above.

20. This question examines Shannon's simplification for  $X_{ab}$  in the preceding excerpt.

Note that Shannon explained the first part of his derivation by saying that 'these reductions were made with 17b using first  $W$ , then  $X$  and  $Y$  as the "X" of 17b.' In fact, it seems that Shannon only used  $W$  and then  $X$  (but not  $Y$ ) as the "X" of 17b. To see this, first recall that Shannon's Identity 17b states the following:

$$X + f(X, Y, \dots Z) = X + f(0, Y, \dots Z) \quad (17b)$$

- (a) We begin by examining how  $W$  is used as the "X" in 17b in Shannon's example above. Let

$$f(W, X, Y, Z, S, V) = W'(X + Y) + (X + Z)(S + W' + Z)(Z' + Y + S'V)$$

and note that this gives us

$$\begin{aligned} X_{ab} &= W + W'(X + Y) + (X + Z)(S + W' + Z)(Z' + Y + S'V) \\ &= W + f(W, X, Y, Z, S, V) \end{aligned}$$

Explain why  $f(0, X, Y, Z, S, V) = (X + Y) + (X + Z)(S + 1 + Z)(Z' + Y + S'V)$ .

Then use 17b to conclude that  $X_{ab} = W + X + Y + (X + Z)(S + 1 + Z)(Z' + Y + S'V)$ .

This completes the first step of Shannon's derivation in the preceding excerpt.

- (b) We now consider how to apply 17b using  $X$  as the "X". Let

$$g(X, Y, Z, S, V) = Y + (X + Z)(S + 1 + Z)(Z' + Y + S'V),$$

so that by the result of part (a), we now have

$$X_{ab} = W + [X + g(X, Y, Z, S, V)]$$

Explain why  $g(0, Y, Z, S, V) = Y + Z(S + 1 + Z)(Z' + Y + S'V)$ .

Then use 17b to conclude that  $X_{ab} = W + X + Y + Z(S + 1 + Z)(Z' + Y + S'V)$ .

Explain why we can now write  $X_{ab} = W + X + Y + Z(Z' + Y + S'V)$ .

Notice that this corresponds to the last line of the first part of Shannon's derivation (just before he multiplied out the last term), suggesting that Shannon actually only used  $W$  and  $X$  (but not  $Y$ ) as the "X" of 17b in this example.

- (c) Finally, we consider how the derivation would look if  $Y$  were used as the "X" in 17b before multiplying the last term out. Let  $h(Y, Z, S, V) = Z(Z' + Y + S'V)$ , so that the expression  $X_{ab} = W + X + Y + Z(S + 1 + Z)(Z' + Y + S'V)$  from part (b) becomes:

$$X_{ab} = W + X + [Y + h(Y, Z, S, V)].$$

Explain why  $h(0, Z, S, V) = Z(Z' + S'V)$ .

Then use 17b to conclude that  $X_{ab} = W + X + Y + Z(Z' + S'V)$ .

Multiply out the last term and compare the result to Shannon's own final result.

21. This question provides a slightly different derivation of Shannon's simplified form for  $X_{ab}$  from the preceding excerpt, where  $X_{ab} = W + W'(X + Y) + (X + Z)(S + W' + Z)(Z' + Y + S'V)$ .
- Begin by letting  $f(W, X, Y, Z, S, V) = W'(X + Y) + (X + Z)(S + W' + Z)(Z' + Y + S'V)$ , so that  $X_{ab} = W + f(W, X, Y, Z, S, V)$ .
  - Explain why  $f(0, X, Y, Z, S, V) = X + Y + (X + Z)(S + 1 + Z)(Z' + Y + S'V)$ .
  - Why can we replace this last expression by  $X + Y + (X + Z)(Z' + Y + S'V)$ ?
  - Use the expression  $f(0, X, Y, Z, S, V) = X + Y + (X + Z)(Z' + Y + S'V)$  in identity 17b to conclude that  $X_{ab} = W + f(W, X, Y, Z, S, V) = W + X + Y + (X + Z)(Z' + Y + S'V)$ .  
(Up to this point, our derivation corresponds essentially to Shannon's first step.)
  - Now let  $g(X, Y, Z, S, V) = Y + (X + Z)(Z' + Y + S'V)$ . Find the value of  $g(0, Y, Z, S, V)$  and use it in identity 17b to conclude that  $X_{ab} = W + X + Y + ZS'V$ .
22. The derivation outlined in project question 21, as well as Shannon's derivation of that same simplified form, both made use of Shannon's identity 17b. Try to obtain this same simplified form by instead using the more standard algebraic process of expansion (i.e., using distributivity of multiplication over addition), beginning with the original expression  $W + W'(X + Y) + (X + Z)(S + W' + Z)(Z' + Y + S'V)$ . Comment on the efficiency of these two approaches.
23. Simplify the following using three applications of 17b (with  $Z$ ,  $X'$ , and  $Y$ ).

$$X_{ab} = Z + Z'(X' + YW'X + WSX + V'Z + X'W')(W + YZ + Y'S) + YZ'$$



## References

- [1] Bocheński, I. M., *A History of Formal Logic*, Thomas, I. (translator & editor), University of Notre Dame Press, Notre Dame, 1961.
- [2] Boole, G., *Mathematical Analysis of Logic*, MacMillan, Barclay & MacMillan, Cambridge, 1847.
- [3] Boole, G., *Mathematical Analysis of Logic*, Open Court, La Salle, 1952.
- [4] Boole, G., *An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities*, Walton and Maberly, London, 1854.
- [5] Boole, G., *An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities*, Dover Publications, , New York, 1958.
- [6] Couturat, C., *The Algebra of Logic*, Robinson, L. G. (translator), Open Court, Chicago, 1914.
- [7] De Morgan, A., *Formal Logic: or, The Calculus of Inference, Necessary and Probable*, Taylor and Walton, London, 1847.
- [8] De Morgan, A., *Trigonometry and Double Algebra*, Taylor, Walton & Maberly, London, 1849.
- [9] Gillispie, C. C., Holmes, F.L., (editors) *Dictionary of Scientific Biography*, Charles Scribner's Sons, New York, 1970.
- [10] Huntington, E. V., Sets of Independent Postulates for the Algebra of Logic, *Transactions of the American Mathematical Society*, 5:3 (1904), 288-309.
- [11] Johnson, W. E., The Logic Calculus. I. General Principles, *Mind*, 1:1 (1892), 3-30.
- [12] Lewis, C. I., *A Survey of Symbolic Logic: The Classic Algebra of Logic*, Dover Publications, New York, 1960.
- [13] Merrill, D., *Augustus De Morgan and the Logic of Relations*, Kluwer, Dordrecht, 1990.
- [14] Shannon, C. E., A Symbolic Analysis of Relay and Switching Circuits, *American Institute of Electrical Engineers Transactions*, 57 (1938), 713-723. Reprinted in [17], 471-495.
- [15] Shannon, C.E., "A Mathematical Theory of Communication," *Bell System Technical Journal*, **27** (1948), 379-423 and 623-656.
- [16] Shannon, C. E., The Synthesis of Two-Terminal Switching Circuits, *Bell System Technical Journal*, 28 (1949), 417-425. Reprinted in [17], 588-627.
- [17] Sloane, N. J. A. & Wyner, A. D. (editors), *Claude Elwood Shannon: Collected Papers*, IEEE Press, New York, 1993.
- [18] Smith, G. C., *The Boole-DeMorgan Correspondence, 1842-1864*, Clarendon Press, Oxford, 1982.
- [19] Venn, J., *Symbolic Logic*, MacMillan, London, 1881.
- [20] Venn, J., *Symbolic Logic*, MacMillan, London, 1894. Reprint Chelsea, Bronx 1971.
- [21] Whitesitt, J. E., *Boolean Algebra and Its Applications*, Addison-Wesley, Reading, 1961. Reprinted by Dover Publications, New York, 1995.

## Notes to the Instructor

This project is designed for an introductory or intermediate course in discrete or finite mathematics that considers boolean algebra from either a mathematical or computer science perspective. The project does assume some (very minimal) familiarity with the set operations of union and intersection. This pre-requisite material may be gained by completing the companion (Boole) project described below, through reading a standard textbook treatment of elementary set operations, or via a short class discussion/lecture. Although no other specific pre-requisite knowledge is necessary for any part of the project, Sections 3 and 4 do assume slightly higher levels of mathematical maturity on the part of the students, roughly commensurate with that of a student who has completed Calculus I (for Section 3) and Calculus II (for Section 4).

Based on an award-winning paper by Claude Shannon, *A Symbolic Analysis of Relay and Switching Circuits*, this project begins with a concise overview of two historical antecedents to Shannon's work. The first of these is George Boole's original work on 'the logic of classes,' included in part to provide students with a connection to another concrete example of a boolean algebra on which they can draw; the second of these is Edward Huntington's work on the axiomatization of boolean algebras, included in part to emphasize to students the relationship between abstract axiomatic structures and concrete models as examples of those structures. Section 2 of the project introduces and develops the use of boolean expressions to represent parallel and series circuits. Within the concrete context of the 2-valued boolean algebra associated with these circuits, the standard properties of a boolean algebra are developed in this section; specific project questions in this section also provide students with practice in using these identities to simplify and manipulate boolean expressions. In Section 3, the concept of a 'disjunctive normal form' for boolean expressions is introduced in the context of circuit design. Section 4 then explores a more sophisticated method for applying boolean algebra to the problem of simplifying complicated circuits.

Since many of the concepts in this project are developed through the exercises, instructors are advised to work through all exercises in advance in order to determine which, if any, she may wish to omit. To complete the project in its entirety requires approximately four 50-minute class periods. Section 4 could easily be omitted for those who wish to have students study only the more fundamental concepts of boolean algebra, or for use with students who do not yet have the necessary level of mathematical maturity for the later sections. Both sections 3 and 4 could also be omitted for similar reasons. Instructors who do elect to complete Section 4 are advised to have students also complete Section 3.

Two other projects on boolean algebra are available as companions to this project, either or both of which could also be used independently of this project. The first companion project "Origins of Boolean Algebra in the Logic of Classes: George Boole, John Venn and C. S. Peirce," is suitable as a preliminary to either the Huntington project or to the Shannon project. Without explicitly introducing modern notation for operations on sets (until the concluding section), that project develops a modern understanding of these operations and their basic properties within the context of early efforts to develop a symbolic algebra for logic. By steadily increasing the level of abstraction, that project also lays the ground work for a more abstract discussion of boolean algebra as a discrete structure, and explores a variety of other mathematical themes, including the notion of an inverse operation, issues related to mathematical notation, and standards of rigor and proof.

The second companion project "Boolean Algebra as an Abstract Structure: Edward V. Huntington and Axiomatization" could be used either as a preliminary to or as a follow-up to the Shannon project on circuit design. That project explores the early axiomatization of boolean algebra as an abstract structure, based on Huntington's 1904 paper *Sets of Independent Postulates for the Algebra of Logic*. In addition to introducing the now standard axioms for the boolean algebra structure, the

project illustrates how to use these postulates to prove some basic properties of boolean algebras. Specific project questions also provide students with practice in using symbolic notation, and encourage them to analyze the logical structure of quantified statements. The project also examines Huntington's use of the two-valued Boolean algebra on  $K = \{0, 1\}$  — first studied by George Boole in his work on the logic of classes — as a model to establish the *independence* and *consistency* of one of his postulate sets. The final section of the project discusses modern (undergraduate) notation and axioms for boolean algebras, and provides several practice exercises to reinforce the ideas developed in the earlier sections.

Implementation with students of any of these projects may be accomplished through individually assigned work, small group work and/or whole class discussion; a combination of these instructional strategies is recommended in order to take advantage of the variety of questions included in the project.



# UNIT 4

## Combinatorics

### 1 Pigeonhole Principle

The Pigeonhole Principle is an obvious but powerful tool in solving many combinatorial problems. We will prove its mathematical form first.

**Theorem 1. [Pigeonhole Principle, PHP]** Let  $A$  be a finite set and let  $f: A \rightarrow \{1, 2, \dots, n\}$  be a function. Let  $p_1, \dots, p_n \in \mathbb{N}$ . If  $|A| > p_1 + \dots + p_n$ , then there exists  $i \in \{1, 2, \dots, n\}$  such that  $|f^{-1}(i)| > p_i$ .

*Proof.* On the contrary, suppose that for each  $i \in \{1, 2, \dots, n\}$ ,  $|f^{-1}(i)| \leq p_i$ . As  $A$  is a disjoint union of the sets  $f^{-1}(i)$ , we have  $|A| = \sum_{i=1}^n |f^{-1}(i)| \leq p_1 + \dots + p_n < |A|$ , a contradiction. ■

The elements of  $A$  are thought of as pigeons and the elements of  $B$  as pigeon holes; so that the principle is commonly formulated in the following forms, which come in handy in particular problems.

**Discussion 2. [Pigeonhole principle (PHP)]**

**PHP1.** If  $n + 1$  pigeons stay in  $n$  holes then there is a hole with at least two pigeons.

**PHP2.** If  $kn + 1$  pigeons stay in  $n$  holes then there is a hole with at least  $k + 1$  pigeons.

**PHP3.** If  $p_1 + \dots + p_n + 1$  pigeons stay in  $n$  holes then there exists  $i, 1 \leq i \leq n$  such that the  $i$ -th hole contains at least  $p_i + 1$  pigeons.

**Example 3. 1.** Consider a tournament of  $n > 1$  players, where each pair plays exactly once and each player wins at least once. Then, there are two players with the same number of wins. **Ans:** Number of wins varies from 1 to  $n - 1$  and there are  $n$  players.

2. A bag contains 5 red, 8 blue, 12 green and 7 yellow marbles. The least number of marbles to be chosen to ensure that there are

- (a) at least 4 marbles of the same color is 13,
- (b) at least 7 marbles of the same color is 24,
- (c) at least 4 red or at least 7 of any other color is 22.

3. In a group of 6 people, prove that there are three mutual friends or three mutual strangers.

**Ans:** Let  $a$  be a person in the group. Let  $F$  be the set of friends of  $a$  and  $S$  the set of strangers to  $a$ . Clearly  $|S| + |F| = 5$ . By PHP either  $|F| \geq 3$  or  $|S| \geq 3$ .

*Case 1:*  $|F| \geq 3$ . If any two in  $F$  are friends then those two along with  $a$  are three mutual friends. Else  $F$  is a set of mutual strangers of size at least 3.

*Case 2:*  $|S| \geq 3$ . If any pair in  $S$  are strangers then those two along with  $a$  are three mutual strangers. Else  $S$  becomes a set of mutual friends of size at least 3.

4. Let  $\{x_1, \dots, x_9\} \subseteq \mathbb{N}$  with  $\sum_{i=1}^9 x_i = 30$ . Then, prove that there exist  $i, j, k \in \{1, 2, \dots, 9\}$  with  $x_i + x_j + x_k \geq 12$ .

**Ans:** Note that  $\frac{\sum_{i=1}^9 x_i}{9} = \frac{30}{9} = 3 + \frac{3}{9}$ . Now use PHP to conclude that there are at least 3  $x_i$ 's that are  $\geq 4$ . Hence, the required result follows.

5. Each point of the plane is colored red or blue, then prove that there exist two points of the same color which are at a distance of 1 unit.

**Ans:** Take a point, say  $P$ . Draw a unit circle with  $P$  as the center. If all the points on the circumference have the same color then we are done. Else, the circumference contains a point which has the same color as that of  $P$ .

6. If 7 points are chosen inside or on the unit circle, then there is a pair of points which are at a distance at most 1.

**Ans:** Divide the circle into 6 equal sectors by drawing radii so that angle between two consecutive radii is  $\pi/3$ . By PHP there is a sector containing at least two points. The distance between these two points is at most 1.

7. If  $n + 1$  integers are selected from  $\{1, 2, \dots, 2n\}$ , then there are two, where one of them divides the other.

**Ans:** Each number has the form  $2^k s$ , where  $s = 2m + 1$  is an odd number. There are  $n$  odd numbers. If we select  $n + 1$  numbers from  $S$ , by PHP some two of them (say,  $x, y$ ) have the same odd part, that is,  $x = 2^i s$  and  $y = 2^j s$ . If  $i \leq j$ , then  $x|y$ , otherwise  $y|x$ .

8. Given any  $n$  integers,  $n \geq 1012$  integers, prove that there is a pair that either differ by, or sum to, a multiple of 2021. Is this true if we replace 1012 by 1011?

**Ans:** Consider some 1012 integers out of the given ones, say,  $n_1, n_2, \dots, n_{1012}$ . Write  $S = \{n_1 - n_k, n_1 + n_k : k = 2, \dots, 1012\}$ . Then,  $|S| = 2022$  and hence, at least two of them will have the same remainder when divided by 2021. Then, consider their difference.

The question in the second part has negative answer. For, consider  $\{0, 1, 2, \dots, 1010\}$ .

9. Prove that there exist two powers of 3 whose difference is divisible by 2021.

**Ans:** Let  $S = \{1 = 3^0, 3, 3^2, 3^3, \dots, 3^{2021}\}$ . Then,  $|S| = 2022$ . As the remainders of any integer when divided by 2021 is  $0, 1, 2, \dots, 2020$ , by PHP, there is a pair which has the same remainder. Hence, 2021 divides  $3^j - 3^i$  for some  $i, j$ .

10. Prove that there exists a power of three that ends with 0001.

**Ans:** Let  $S = \{1 = 3^0, 3, 3^2, 3^3, \dots\}$ . Now, divide each element of  $S$  by  $10^4$ . As  $|S| > 10^4$ , by PHP, there exist  $i > j$  such that the remainders of  $3^i$  and  $3^j$ , when divided by  $10^4$ , are equal. But  $\gcd(10^4, 3) = 1$  and thus,  $10^4$  divides  $3^\ell - 1$ . Then  $3^\ell - 1 = s \cdot 10^4$  for some positive integer  $s$ . That is,  $3^\ell = s \cdot 10^4 + 1$  from which the result follows.

11. Suppose that  $f(x)$  is a polynomial with integer coefficients. If  $f(x) = 5$  for three distinct integers, then for no integer  $x$ ,  $f(x)$  can be equal to 4.

**Ans:** Let  $f(x) = 5$ , for  $x \in \{a, b, c\}$ . If  $f(d) = 4$ , for an integer  $d$ , then  $(d - a)|f(d) - f(a) = -1$ . So,  $a = d \pm 1$ . Similarly  $b, c = d \pm 1$ . By PHP two of  $a, b, c$  are the same, a contradiction.

**Alternate.** If  $f$  is an integer polynomial and  $f(m) = 0$  for some integer  $m$ , then using the factor/remainder theorem  $f(x) = (x - m)g(x)$  for some integer polynomial  $g$ . For our problem, we see that  $f(x) = (x - a)(x - b)(x - c)g(x) + 5$ , where  $g$  is an integer polynomial. If  $f(n) = 4$ , then  $(n - a), (n - b), (n - c) \equiv -1 \pmod{5}$ , so that  $(n - a), (n - b), (n - c) \in \{1, -1\}$ . By PHP some two of them are the same, a contradiction.

**Theorem 4.** Let  $r_1, r_2, \dots, r_{mn+1}$  be a sequence of  $mn + 1$  distinct real numbers. Then, prove that there is a subsequence of  $m + 1$  numbers which is increasing or there is a subsequence of  $n + 1$  numbers which is decreasing.

Does the above statement hold for every collection of  $mn$  distinct numbers?

*Proof.* Define  $l_i$  to be the maximum length of an increasing subsequence starting at  $r_i$ . If some  $l_i \geq m + 1$  then we have nothing to prove. So, let  $1 \leq l_i \leq m$ . Since  $(l_i)$  is a sequence of  $mn + 1$  integers, by PHP, there is one number which repeats at least  $n + 1$  times. Let  $l_{i_1} = l_{i_2} = \dots = l_{i_{n+1}} = s$ , where  $i_1 < i_2 < \dots < i_{n+1}$ . Notice that  $r_{i_1} > r_{i_2}$ , because if  $r_{i_1} < r_{i_2}$ , then ' $r_{i_1}$ ' together with the increasing sequence of length  $s$  starting with  $r_{i_2}$ ' gives an increasing sequence of length  $s + 1$ . Similarly,  $r_{i_2} > r_{i_3} > \dots > r_{i_{n+1}}$  and hence the required result holds.

**Alternate.** Let  $S = \{r_1, r_2, \dots, r_{mn+1}\}$  and define a map  $f : S \rightarrow \mathbb{Z} \times \mathbb{Z}$  by  $f(r_i) = (s, t)$ , for  $1 \leq i \leq mn + 1$ , where  $s$  equals the length of the largest increasing subsequence starting with  $r_i$  and  $t$  equals the length of the largest decreasing subsequence ending at  $r_i$ . Now, if either  $s \geq m + 1$  or  $t \geq n + 1$ , we are done. If not, then note that  $1 \leq s \leq m$  and  $1 \leq t \leq n$ . So, the number of tuples  $(s, t)$  is at most  $mn$ . Thus, the  $mn + 1$  distinct numbers are being mapped to  $mn$  tuples and hence by PHP there are two numbers  $r_i \neq r_j$  such that  $f(r_i) = f(r_j)$ . Now, proceed as in the previous case to get the required result.

The above statement is FALSE. Consider the sequence:

$$n, n - 1, \dots, 1, 2n, 2n - 1, \dots, n + 1, 3n, 3n - 1, \dots, 2n + 1, \dots, mn, mn - 1, \dots, mn - n + 1.$$

■

**Theorem 5.** Corresponding to each irrational number  $a$ , there exist infinitely many rational numbers  $\frac{p}{q}$  such that  $|a - \frac{p}{q}| < \frac{1}{q^2}$ .

*Proof.* It is enough to show that there are infinitely many  $(p, q) \in \mathbb{Z}^2$  with  $|qa - p| < \frac{1}{q}$ . As  $a$  is irrational, for every  $m \in \mathbb{N}$ ,  $0 < ia - [ia] < 1$ , for  $i = 1, \dots, m + 1$ . Hence, by PHP there exist  $i, j$  with  $i < j$  such that

$$|(j - i)a - ([ja] - [ia])| < \frac{1}{m} \leq \frac{1}{j - i}.$$

Then, the pair  $(p_1, q_1) = ([ja] - [ia], j - i)$  satisfies the required property. To generate another pair, find  $m_2$  such that

$$\frac{1}{m_2} < |a - \frac{p_1}{q_1}|$$

and proceed as before to get  $(p_2, q_2)$  such that  $|q_2a - p_2| < \frac{1}{m_2} \leq \frac{1}{q_2}$ . Since  $|a - \frac{p_2}{q_2}| < \frac{1}{m_2} < |a - \frac{p_1}{q_1}|$ , we have  $\frac{p_1}{q_1} \neq \frac{p_2}{q_2}$ . Now use induction to get the required result. ■

**Theorem 6.** Let  $\alpha$  be a positive irrational number. Then prove that  $S = \{m + n\alpha : m, n \in \mathbb{Z}\}$  is dense in  $\mathbb{R}$ .

*Proof.* Consider any open interval  $(a, b)$ . By Archimedean property, there exists  $n \in \mathbb{N}$  such that  $\frac{1}{n} < b - a$ . Observe that  $0 < r_k = k\alpha - [k\alpha] < 1$ ,  $k = 1, \dots, n + 1$ . By PHP, some two satisfy

$0 < r_i - r_j < 1/n$ . Then  $x = r_i - r_j = (i - j)\alpha + ([j\alpha] - [i\alpha]) \in S$ . Let  $p$  be the smallest integer so that  $px > a$ . If  $px \geq b$ , then  $(a, b) \subseteq ((p - 1)x, px)$  and so  $b - a \leq x < \frac{1}{n}$ , which is not possible. So,  $px \in (a, b)$  and  $px \in S$  as well. Thus,  $(a, b) \cap S \neq \emptyset$ . ■

**EXERCISE 71.** Consider the poset  $(X = \mathcal{P}(\{1, 2, 3, 4\}), \subseteq)$ . Write 6 maximal chains  $P_1, \dots, P_6$  (need not be disjoint) such that  $\bigcup_i P_i = X$ . Let  $A_1, \dots, A_7$  be 7 distinct subsets of  $\{1, 2, 3, 4\}$ . Use PHP, to prove that there exist  $i, j$  such that  $A_i, A_j \in P_k$ , for some  $k$ . That is,  $\{A_1, \dots, A_7\}$  cannot be an anti-chain. Conclude that this holds as the width of the poset is 6.

2. Suppose that  $f(x)$  is a polynomial with integer coefficients. If
  - (a)  $f(x) = 14$  for three distinct integers, then for no integer  $x$ ,  $f(x)$  can be equal to 15.
  - (b)  $f(x) = 11$  for five distinct integers, then for no integer  $x$ ,  $f(x)$  can be equal to 9.
3. There are 7 distinct real numbers. Is it possible to select two of them, say  $x$  and  $y$  such that  $0 < \frac{x-y}{1+xy} < \frac{1}{\sqrt{3}}$ ?
4. If  $n$  is odd then for any permutation  $p$  of  $\{1, 2, \dots, n\}$  the product  $\prod_{i=1}^n (i - p(i))$  is even.
5. Five points are chosen at the nodes of a square lattice (view  $\mathbb{Z} \times \mathbb{Z}$ ). Why is it certain that a mid-point of some two of them is a lattice point?
6. Choose 5 points at random inside an equilateral triangle of side 2 units. Show that there exist two points that are away from each other by at most 1 unit.
7. Take 25 points on a plane satisfying 'among any three of them there is a pair at a distance less than 1'. Then, some circle of unit radius contains at least 13 of the given points.
8. If each point of a circle is colored either red or blue, then show that there exists an isosceles triangle with vertices of the same color.
9. Each point of the plane is colored red or blue, then prove the following.
  - (a) There is an equilateral triangle all of whose vertices have the same color.
  - (b) There is a rectangle all of whose vertices have the same color.
10. Show that among any 6 integers from  $\{1, 2, \dots, 10\}$ , there exists a pair with odd sum.
11. Any 14-subset of  $\{1, 2, \dots, 46\}$  has four elements  $a, b, c, d$  such that  $a + b = c + d$ .
12. Show that if 9 of the 12 chairs in a row are filled, then some 3 consecutive chairs are filled. Will 8 work?
13. Show that every  $n$ -sequence of integers has a consecutive subsequence with sum divisible by  $n$ .
14. Let  $n > 3$  and  $S \subseteq \{1, 2, \dots, n\}$  of size  $m = \lfloor \frac{n+2}{2} \rfloor + 1$ . Then, there exist  $a, b, c \in S$  such that  $a + b = c$ .
15. Let  $a, b \in \mathbb{N}$ ,  $a < b$ . Given more than half of the integers in the set  $\{1, 2, \dots, a + b\}$ , there is a pair which differ by either  $a$  or  $b$ .
16. Consider a chess board with two of the diagonally opposite corners removed. Is it possible to cover the board with pieces of rectangular dominoes whose size is exactly two board squares?
17. Mark the centers of all squares of an  $8 \times 8$  chess board. Is it possible to cut the board with 13 straight lines not passing through any center, so that every piece had at most 1 center?
18. Fifteen squirrels have 104 nuts. Then, some two squirrels have equal number of nuts.

19. Let  $\{x_1, x_2, \dots, x_n\} \subseteq \mathbb{Z}$ . Prove that there exist  $1 \leq i \leq j \leq n$  such that  $x_i + x_{i+1} + \dots + x_{j-1} + x_j$  is a multiple of 2021, whenever  $n \geq 2021$ .
20. Let  $A$  and  $B$  be two discs, each having  $2n$  equal sectors. On disc  $A$ ,  $n$  sectors are colored red and  $n$  are colored blue. The sectors of disc  $B$  are colored arbitrarily with red and blue colors. Show that there is a way of putting the two discs, one above the other, so that at least  $n$  corresponding sectors have the same colors.
21. Show that there is a non-zero integer multiple of  $\sqrt{2021}$  whose decimal representation has 2022 consecutive zeroes after the first decimal point.
22. If more than half of the subsets of  $\{1, 2, \dots, n\}$  are selected, then some two of the selected subsets have the property that one is a subset of the other.
23. Suppose we are given any ten 4-subsets of  $\{1, 2, \dots, 11\}$ . Then, show that some two of them have at least 2 elements in common.
24. A person takes at least one aspirin a day for 30 days. If he takes 45 aspirin altogether then prove that in some sequence of consecutive days he takes exactly 14 aspirins.
25. If 58 entries of a  $14 \times 14$  matrix are 1 and the remaining entries are 0, then prove that there is a  $2 \times 2$  submatrix with all entries 1.
26. Let  $A$  and  $B$  be two finite non-empty sets with  $B = \{b_1, b_2, \dots, b_m\}$ . Let  $f : A \rightarrow B$  be any function. Then, for any non-negative integers  $a_1, a_2, \dots, a_m$  if  $|A| = a_1 + a_2 + \dots + a_m - m + 1$  then prove that there exists an  $i, 1 \leq i \leq m$  such that  $|f^{-1}(b_i)| \geq a_i$ .
27. Each of the given 9 lines cuts a given square into two quadrilaterals whose areas are in the ratio 2 : 3. Prove that at least three of these lines pass through the same point.
28. Let  $S \subseteq \{1, 2, \dots, 100\}$  be a 10-set. Then, some two disjoint subsets of  $S$  have equal sum.
29. Prove that corresponding to each  $n \in \mathbb{N}$ ,  $n$  odd, there exists an  $\ell \in \mathbb{N}$  such that  $n$  divides  $2^\ell - 1$ .
30. Does there exist a multiple of 2021 that is formed using only the digits
  - (a) 2? Justify your answer.
  - (b) 2 and 3 and the number of 2's and 3's are equal? Justify your answer.
31. Each natural number has a multiple of the form  $9 \dots 90 \dots 0$ , with at least one 9.

## 6.2 Principle of Inclusion and Exclusion

We start this section with the following example.

**Example 1.** How many natural numbers  $n \leq 1000$  are not divisible by any of 2, 3?

**Ans:** Let  $A_2 = \{n \in \mathbb{N} | n \leq 1000, 2|n\}$  and  $A_3 = \{n \in \mathbb{N} | n \leq 1000, 3|n\}$ . Then,  $|A_2 \cup A_3| = |A_2| + |A_3| - |A_2 \cap A_3| = 500 + 333 - 166 = 667$ . So, the required answer is  $1000 - 667 = 333$ .

We now generalize the above idea whenever we have 3 or more sets.

**Theorem 2. [Principle of Inclusion and Exclusion, PIE]** Let  $A_1, \dots, A_n$  be finite subsets of a set  $U$ . Then,

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{k=1}^n (-1)^{k+1} \left[ \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| \right].$$



Or equivalently, the number of elements of  $U$  which are in none of  $A_1, A_2, \dots, A_n$  equals

$$|U \setminus \bigcup_{i=1}^n A_i| = |U| - \sum_{k=1}^n (-1)^k \left[ \sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}| \right].$$

*Proof.* Let  $x \notin \bigcup_{i=1}^n A_i$ . Then, we show that inclusion of  $x$  in some  $A_i$  contributes (increases the value) 1 to both sides of Equation (6.1). So, assume that  $x$  is included only in the sets  $A_1, \dots, A_r$ . Then, the contribution of  $x$  to  $|A_{i_1} \cap \dots \cap A_{i_k}|$  is 1 if and only if  $\{i_1, \dots, i_k\} \subseteq \{1, 2, \dots, r\}$ . Hence, the contribution of  $x$  to  $\sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}|$  is  $C(r, k)$ . Thus, the contribution of  $x$  to the right hand side of Equation (6.1) is

$$C(r, 1) - C(r, 2) + C(r, 3) - \dots + (-1)^{r+1} C(r, r) = 1.$$

The element  $x$  clearly contributes 1 to the left hand side of Equation (6.1) and hence the required result follows. The proof of the equivalent condition is left for the readers. ■

**Example 3.** How many integers between 1 and 10000 are divisible by none of 2, 3, 5, 7?

**Ans:** For  $i \in \{2, 3, 5, 7\}$ , let  $A_i = \{n \in \mathbb{N} | n \leq 10000, i|n\}$ . Therefore, the required answer is  $10000 - |A_2 \cup A_3 \cup A_5 \cup A_7| = 2285$ .

**Definition 4. [Euler Totient Function]** For a fixed  $n \in \mathbb{N}$ , the **Euler's totient function** is defined as  $\varphi(n) = |\{k \in \mathbb{N} : k \leq n, \gcd(k, n) = 1\}|$ .

Thus,  $\varphi(n)$  is the number of natural numbers less than or equal to  $n$  and relatively prime to  $n$ . For instance,  $\varphi(1) = 1$ ,  $\varphi(2) = 1$ ,  $\varphi(3) = 2$ ,  $\varphi(4) = 3$ ,  $\varphi(12) = 4$ , etc.

**Theorem 5.** Let  $p_1, \dots, p_k$  be the distinct prime divisors of  $n$ . Then

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

*Proof.* For  $1 \leq i \leq k$ , let  $A_i = \{m \in \mathbb{N} : m \leq n, p_i | m\}$ . Then,  $|A_i| = \frac{n}{p_i}$ ,  $|A_i \cap A_j| = \frac{n}{p_i p_j}$ , and so on. By PIE,

$$\begin{aligned} \varphi(n) &= n - |\bigcup_i A_i| = n \left[ 1 - \sum_{i=1}^k \frac{1}{p_i} + \sum_{1 \leq i < j \leq k} \frac{1}{p_i p_j} - \dots + (-1)^k \frac{1}{p_1 p_2 \dots p_k} \right] \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

**Definition 6. [Derangement]** A **derangement** of objects in a finite set  $S$  is a permutation/arrangement  $\sigma$  on  $S$  such that for each  $x, \sigma(x) \neq x$ . The number of derangements of  $\{1, 2, \dots, n\}$  is denoted by  $D_n$  with the convention that  $D_0 = 1$ .

For example, 2, 1, 4, 3 is a derangement of 1, 2, 3, 4, but 2, 3, 1, 4 is not a derangement of 1, 2, 3, 4.

If a sequence  $(x_n)$  converges to some limit  $\ell$ , we say that  $x_n$  is approximately  $\ell$  for large values of  $n$ , and write  $x_n \approx \ell$ .

**Theorem 7.** For  $n \in \mathbb{N}$ ,  $D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$ . Consequently,  $\frac{D_n}{n!} \approx \frac{1}{e}$ .

*Proof.* For each  $i$ ,  $1 \leq i \leq n$ , let  $A_i$  be the set of arrangements  $\sigma$  such that  $\sigma(i) = i$ . Then, verify that  $|A_i| = (n-1)!$ ,  $|A_i \cap A_j| = (n-2)!$  and so on. Thus,

$$|\cup_i A_i| = n.(n-1)! - C(n, 2)(n-2)! + \dots + (-1)^{n-1}C(n, n)0! = n! \sum_{k=1}^n \frac{(-1)^{k-1}}{k!}.$$

So,  $D_n = n! - |\cup_i A_i| = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$ . Since  $\sum_{k=0}^{\infty} \frac{(-1)^k}{k!} = e^{-1}$ , it follows that  $\lim_{n \rightarrow \infty} \frac{D_n}{n!} = \frac{1}{e}$ . ■

**Example 8.** How many square-free integers do not exceed  $n$  for a given  $n \in \mathbb{N}$ ?

Answer: Let  $P = \{p_1, \dots, p_s\}$  be the set of primes not exceeding  $\sqrt{n}$  and for  $1 \leq i \leq s$ , let  $A_i$  be the set of integers between 1 and  $n$  that are multiples of  $p_i^2$ . Then

$$|A_i| = \left\lfloor \frac{n}{p_i^2} \right\rfloor, \quad |A_i \cap A_j| = \left\lfloor \frac{n}{p_i^2 p_j^2} \right\rfloor, \quad \dots$$

So, the number of square-free integers not greater than  $n$  is

$$n - |\cup_{i=1}^s A_i| = n - \sum_{i=1}^s \left\lfloor \frac{n}{p_i^2} \right\rfloor + \sum_{1 \leq i < j \leq s} \left\lfloor \frac{n}{p_i^2 p_j^2} \right\rfloor - \sum_{1 \leq i < j < k \leq s} \left\lfloor \frac{n}{p_i^2 p_j^2 p_k^2} \right\rfloor + \dots$$

For  $n = 100$ , we have  $P = \{2, 3, 5, 7\}$ . So, the number of square-free integers not exceeding 100 is

$$100 - \left\lfloor \frac{100}{4} \right\rfloor - \left\lfloor \frac{100}{9} \right\rfloor - \left\lfloor \frac{100}{25} \right\rfloor - \left\lfloor \frac{100}{49} \right\rfloor + \left\lfloor \frac{100}{36} \right\rfloor + \left\lfloor \frac{100}{100} \right\rfloor = 61.$$

**EXERCISE 9. 1.** In a school there are 12 students who take an art course  $A$ , 20 who take a biology course  $B$ , 20 who take a chemistry course  $C$  and 8 who take a dance course  $D$ . There are 5 students who take both  $A$  and  $B$ , 7 students who take both  $A$  and  $C$ , 4 students who take both  $A$  and  $D$ , 16 students who take both  $B$  and  $C$ , 4 students who take both  $B$  and  $D$  and 3 students who take both  $C$  and  $D$ . There are 3 who take  $A$ ,  $B$  and  $C$ ; 2 who take  $A$ ,  $B$  and  $D$ ; 3 who take  $A$ ,  $C$  and  $D$ ; and 2 who take  $B$ ,  $C$  and  $D$ . Finally there are 2 in all four courses and further 71 students who have not taken any of these courses. Find the total number of students.

2. Let  $n \in \mathbb{N}$ . Using PIE, show that  $S(n, r) = \frac{1}{r!} \sum_{i=0}^{r-1} (-1)^i C(r, i) (r-i)^n$ .

3. Show that  $\sum_{k=0}^m (-1)^k C(m, k) (m-k)^n = \begin{cases} n! & \text{if } m = n \\ 0 & \text{if } m > n. \end{cases}$

4. Determine the number of 10-letter words over English alphabet that do not contain all the vowels.

5. Let  $m, n \in \mathbb{N}$  with  $\gcd(m, n) = 1$ . Prove that  $\varphi(mn) = \varphi(m)\varphi(n)$ .

6. Determine all natural numbers  $n$  satisfying  $\varphi(n) = 13$ .

7. Determine all natural numbers  $n$  satisfying  $\varphi(n) = 12$ .

8. For each fixed  $n \in \mathbb{N}$ , use mathematical induction to prove that  $\sum_{d|n} \varphi(d) = n$ .

9. For each fixed  $n \in \mathbb{N}$ , use mathematical induction to prove that  $\sum_{d|n} \varphi(d) = n$ .

10. A function  $f : \mathbb{N} \rightarrow \mathbb{N}$  is said to be **multiplicative** if  $f(nm) = f(n)f(m)$ , whenever  $\gcd(n, m) = 1$ . Let  $f, g : \mathbb{N} \rightarrow \mathbb{N}$  be functions satisfying  $f(n) = \sum_{d|n} g(d)$  and  $f(1) = g(1) = 1$ . If  $f$  is multiplicative then use induction to show that  $g$  is also multiplicative.

11. Show that for  $n \geq 2$ ,  $D_n = \lfloor \frac{n!}{e} + \frac{1}{2} \rfloor$ .
12. Prove combinatorially:  $\sum_{i=0}^n C(n, i) D_{n-i} = n!$ .
13. Find the number of non-negative integer solutions of  $a + b + c + d = 27$ , where  $1 \leq a \leq 5$ ,  $2 \leq b \leq 7$ ,  $3 \leq c \leq 9$ ,  $4 \leq d \leq 11$ .
14. Let  $x$  be a natural number less than or equal to 9999999.
  - (a) Find the number of  $x$ 's for which the sum of the digits in  $x$  equals 30.
  - (b) How many of the solutions obtained in the first part consist of 7 digits?
15. In how many ways the digits  $0, 1, \dots, 9$  can be arranged so that the digit  $i$  is never followed immediately by  $i + 1$ .
16. Determine the number of strings of length 15 that use some or all of the digits  $0, 1, \dots, 9$ , so that no string contains all the 10 digits.
17. Determine the number of ways of permuting the 26 letters of the English alphabet so that none of the patterns *lazy*, *run*, *show* and *pet* occurs.
18. Let  $S = \{(n_1, n_2, n_3) | n_i \in \mathbb{N}, \sum n_i = 15\}$ . Evaluate  $\sum_{(n_1, n_2, n_3) \in S} \frac{15!}{n_1! n_2! n_3!}$ .
19. Each of the 9 senior students said: 'the number of junior students I want to help is exactly one'. There were 4 junior students  $a, b, c, d$ , who wanted their help. The allocation was done randomly. What is the probability that either  $a$  has exactly two seniors to help him or  $b$  has exactly 3 seniors to help him or has no seniors to help him?

## Generating Functions

This is one of the strongest tools in combinatorics. We start with the definition of formal power series over  $\mathbb{Q}$  and develop the theory of generating functions. This is then used to get closed form expressions for some known recurrence relations and are then further used to get some binomial identities.

**Definition 1.1.** 1. An algebraic expression of the form  $f(x) = \sum_{n \geq 0} a_n x^n$ , where  $a_n \in \mathbb{Q}$  for all  $n \geq 0$ , is called a **formal power series** in the indeterminate  $x$  over  $\mathbb{C}$  and is denoted by  $\mathbb{Q}[[x]]$ .

By  $\text{CF}[x^n, f]$ , we denote the coefficient of  $x^n$  in  $f$ , e.g.,  $\text{CF}\left[x^n, \sum_{n \geq 0} a_n x^n\right] = a_n$ .

2. Two elements  $f, g \in \mathbb{Q}[[x]]$  are said to be equal if  $\text{CF}[x^n, f] = \text{CF}[x^n, g]$  for all  $n \geq 0$ .
3. Let  $f(x) = \sum_{n \geq 0} a_n x^n$  and  $g(x) = \sum_{n \geq 0} b_n x^n$  be elements in  $\mathbb{Q}[[x]]$ . Then, their

- (a) sum/addition is defined by  $\text{CF}[x^n, f + g] = \text{CF}[x^n, f] + \text{CF}[x^n, g]$ .
- (b) scalar multiplication is defined by  $\text{CF}[x^n, \alpha f] = \alpha \text{CF}[x^n, f]$ .

Thus, with the above operations, the class of formal power series  $\mathbb{Q}[[x]]$  over  $\mathbb{Q}$ , is a vector space which is isomorphic to the space of all sequences.

- (c) One also defines the product (called the **Cauchy product**) by  $\text{CF}[x^n, f \cdot g] = c_n = \sum_{k=0}^n a_k b_{n-k}$ .

Before proceeding further, we consider the following examples.

**Example 3.2.1.** How many words of size 8 can be formed with 6 copies of  $A$  and 6 copies of  $B$ ?

**Ans:**  $\sum_{k=2}^6 C(8, k)$ , as we just need to choose  $k$  places for  $A$ , where  $2 \leq k \leq 6$ .

**Alternate.** In any such word, we need  $m$  many  $A$ 's and  $n$  many  $B$ 's with  $m + n = 8$ ,  $m \leq 6$  and  $n \leq 6$ . Also, the number of words with  $m$  many  $A$ 's and  $n$  many  $B$ 's is  $\frac{8!}{m!n!}$ .

We identify this number with  $\frac{8!x^m y^n}{m!n!}$  and note that this is a term of degree 8 in

$$8! \left[ 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} \right] \left[ 1 + y + \frac{y^2}{2!} + \frac{y^3}{3!} + \frac{y^4}{4!} + \frac{y^5}{5!} + \frac{y^6}{6!} \right].$$

If we replace  $y$  by  $x$ , then our answer is

$$\begin{aligned} & 8! \text{CF} \left[ x^8, \left( 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} \right) \left( 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} \right) \right] \\ = & 8! \text{CF} \left[ x^8, \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} \right) \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} \right) \right] \\ = & 8! \text{CF} \left[ x^8, \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right) \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right) \right] \\ = & 8! \text{CF} \left[ x^8, (e^x - 1 - x)^2 = e^{2x} + 1 + x^2 - 2xe^x - 2e^x + 2x \right] = 8! \left( \frac{2^8}{8!} - \frac{2}{7!} - \frac{2}{8!} \right) = 238. \end{aligned}$$

2. How many anagrams (rearrangements) are there of the word *MISSISSIPPI*?

**Ans:** Using basic counting, the answer is  $\frac{11!}{4!4!2!}$ .

**Alternate.** For another understanding, note that  $\frac{11!}{4!4!2!} = 11! \times \text{CF} \left[ x^{11}, x \frac{x^4}{4!} \frac{x^4}{4!} \frac{x^2}{2!} \right]$ . Here the numbers  $1 = \text{CF}[x, x]$ ,  $\frac{1}{4!} = \text{CF} \left[ x^4, \frac{x^4}{4!} \right]$ ,  $\frac{1}{4!} = \text{CF} \left[ x^4, \frac{x^4}{4!} \right]$  and  $\frac{1}{2!} = \text{CF} \left[ x^2, \frac{x^2}{2!} \right]$  correspond to the number of occurrences of  $M, I, S$  and  $P$ , respectively. Hence, the readers should note that

$$\begin{aligned} \frac{11!}{4!4!2!} &= 11! \text{CF} \left[ x^{11}, (1+x) \left( 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} \right)^2 \left( 1 + x + \frac{x^2}{2!} \right) \right], \text{ or} \\ \frac{11!}{4!4!2!} &= 11! \text{CF} \left[ x^{11}, \left( x + \frac{x^2}{2!} + \dots \right) \left( \frac{x^4}{4!} + \frac{x^5}{5!} + \dots \right)^2 \left( \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right) \right] \end{aligned}$$

3. How many multi-subsets of size 4 of the multiset  $\{E, X, A, M, I, N, A, T, I, O, N\}$  are there?

**Ans:** By direct counting the answer is

$$\begin{aligned} & C(5, 4) + C(5, 3)C(3, 1) + [C(5, 2)C(3, 2) + C(5, 2)C(3, 1)] \\ & + [C(5, 1)C(3, 3) + C(5, 1)C(3, 1)C(2, 1)] + [C(5, 0)C(3, 2) + C(5, 0)C(3, 1)] = 136. \end{aligned}$$

**Alternate.** It is as good as asking how many  $A$ 's are you including and how many  $E$ 's, etc. Suppose that we are considering  $A^2EM$  (means  $\{A, A, E, M\}$ ). But this is a term of degree 4 in

$$(1 + A + A^2)(1 + E)(1 + I + I^2)(1 + M)(1 + N + N^2)(1 + O)(1 + T)(1 + X).$$

So their number is nothing but

$$\begin{aligned} & \text{CF} \left[ x^4, (1+x)^5 (1+x+x^2)^3 \right] = \\ & \text{CF} \left[ x^4, (1+5x+10x^2+10x^3+5x^4+\dots)(1+3x+6x^2+7x^3+6x^4+\dots) \right] = 136. \end{aligned}$$

4. How many non-negative integer solutions of  $u + v + w + t = 10$  are there?

**Ans:** Note that  $u$  can take any value from 0 to 10 which corresponds to  $1 + x + \dots + x^{10}$ . Hence, the required answer is

$$\text{CF}[x^{10}, (1 + x + x^2 + \dots)^4 = (1 - x)^{-4}] = C(13, 10) = \frac{4 \cdot 5 \cdot \dots \cdot 13}{10!}.$$

**Definition 6.3.3. [Generating Functions]** Let  $(b_n) = (b_0, b_1, b_2, \dots)$  be a sequence of integers. Then,

1. the **ordinary generating function (ogf)** is the formal power series

$$b_0 + b_1x + b_2x^2 + b_3x^3 + \dots, \text{ and}$$

2. the **exponential generating function (egf)** is the formal power series

$$b_0 + b_1x + b_2\frac{x^2}{2!} + b_3\frac{x^3}{3!} + \dots.$$

If the sequence has finitely many elements then the generating functions have finitely many terms.

**Example 6.3.4.** What is the number of non-negative integer solutions of  $2a + 3b + 5c = r$ ,  $r \in \mathbb{N}_0$ ?

**Ans:** Note that  $a \in \mathbb{N}_0$  and hence  $2a$  corresponds to the formal power series  $1 + x^2 + x^4 + \dots$ . Thus, we need to consider the ogf

$$(1 + x^2 + x^4 + \dots)(1 + x^3 + x^6 + \dots)(1 + x^5 + x^{10} + \dots) = \frac{1}{(1 - x^2)(1 - x^3)(1 - x^5)}.$$

Hence, the required answer is  $\text{CF}\left[x^r, \frac{1}{(1 - x^2)(1 - x^3)(1 - x^5)}\right]$ .

**Remark 3.5.** 1. Let  $f(x) = \sum_{n \geq 0} a_n \frac{x^n}{n!}$ ,  $g(x) = \sum_{n \geq 0} b_n \frac{x^n}{n!} \in \mathbb{Q}[[x]]$ . Then, in case of egf, their product equals  $\sum_{n \geq 0} d_n \frac{x^n}{n!}$ , where  $d_n = \sum_{k=0}^n C(n, k) a_k b_{n-k}$ , for  $n \geq 0$ .

2. Note that  $e^{e^x - 1} \in \mathbb{Q}[[x]]$  as  $e^y = \sum_{n \geq 0} \frac{y^n}{n!}$  implies that  $e^{e^x - 1} = \sum_{n \geq 0} \frac{(e^x - 1)^n}{n!}$  and

$$\text{CF}[x^m, e^{e^x - 1}] = \text{CF}\left[x^m, \sum_{n \geq 0} \frac{(e^x - 1)^n}{n!}\right] = \sum_{n=0}^m \text{CF}\left[x^m, \frac{(e^x - 1)^n}{n!}\right]. \quad (6.2)$$

That is, for each  $m \geq 0$ ,  $\text{CF}[x^m, e^{e^x - 1}]$  is a sum of a finite number of rational numbers. Whereas, the expression  $e^{e^x} \notin \mathbb{Q}[[x]]$  as computing  $\text{CF}[x^m, e^{e^x}]$ , for all  $m \geq 0$ , requires infinitely many computations.

3. Recall that if  $f(x) = \sum_{n \geq 0} a_n x^n$ ,  $g(x) = \sum_{n \geq 0} b_n x^n \in \mathbb{Q}[[x]]$  then the composition

$$(f \circ g)(x) = f(g(x)) = \sum_{n \geq 0} a_n (g(x))^n = \sum_{n \geq 0} a_n \left(\sum_{m \geq 0} b_m x^m\right)^n$$

may not be defined (just to compute the constant term of the composition, one may have to look at an infinite sum of rational numbers). For example, let  $f(x) = e^x$  and  $g(x) = x + 1$ . Note that  $g(0) = 1 \neq 0$ . Here,  $(f \circ g)(x) = f(g(x)) = f(x + 1) = e^{x+1}$ . So, as function  $f \circ g$  is well defined, but there is no formal procedure to write  $e^{x+1}$  as  $\sum_{k \geq 0} a_k x^k \in \mathbb{Q}[[x]]$  (i.e., with  $a_k \in \mathbb{Q}$ ) and hence  $e^{x+1}$  is not a formal power series over  $\mathbb{Q}$ .

With the algebraic operations as defined in Definition 6.3.1.3, it can be checked that  $\mathbb{Q}[[x]]$  forms a Commutative Ring with identity, where the identity element is given by the formal power series  $f(x) = 1$ . In this ring, the element  $f(x) = \sum_{n \geq 0} a_n x^n$  is said to have a **reciprocal** if there exists another element  $g(x) = \sum_{n \geq 0} b_n x^n \in \mathbb{Q}[[x]]$  such that  $f(x) \cdot g(x) = 1$ . So, the question arises, under what conditions on  $\text{CF}[x^n, f]$ , can we find  $g(x) \in \mathbb{Q}[[x]]$  such that  $f(x)g(x) = 1$ . The answer to this question is given in the following proposition.

**Proposition 3.6.** *The reciprocal of  $f \in \mathbb{Q}[[x]]$  exists if and only if  $\text{CF}[x^0, f] \neq 0$ . Further, if  $a_n \in \mathbb{Q}$ , for all  $n$  then  $a_n \in \mathbb{Q}$ , for all  $n$ .*

*Proof.* Let  $g(x) = \sum_{n \geq 0} b_n x^n \in \mathbb{Q}[[x]]$  be the reciprocal of  $f(x) = \sum_{n \geq 0} a_n x^n$ . Then,  $f(x)g(x) = 1$  if and only if  $\text{CF}[x^0, f \cdot g] = 1$  and  $\text{CF}[x^n, f \cdot g] = 0$ , for all  $n \geq 1$ .

But, by definition of the Cauchy product,  $\text{CF}[x^0, f \cdot g] = a_0 b_0$ . Hence, if  $a_0 = \text{CF}[x^0, f] = 0$  then  $\text{CF}[x^0, f \cdot g] = 0$  and thus,  $f$  cannot have a reciprocal. However, if  $a_0 \neq 0$ , then the coefficients  $\text{CF}[x^n, g] = b_n$ 's can be recursively obtained as follows:

$$b_0 = 1/a_0 \text{ as } 1 = c_0 = a_0 b_0;$$

$$b_1 = -(a_1 b_0)/a_0 \text{ as } 0 = c_1 = a_0 b_1 + a_1 b_0;$$

$b_2 = -(a_2 b_0 + a_1 b_1)/a_0$  as  $0 = c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$ ; and in general, if we have computed  $b_k$ , for  $k \leq r$ , then using  $0 = c_{r+1} = a_{r+1} b_0 + a_r b_1 + \dots + a_1 b_r + a_0 b_{r+1}$ , we get

$$b_{r+1} = -(a_{r+1} b_0 + a_r b_1 + \dots + a_1 b_r)/a_0.$$

Hence, the required result follows. ■

The next result gives the condition under which the composition  $(f \circ g)(x)$  is well defined.

**Proposition 3.7.** *Let  $f, g \in \mathbb{Q}[[x]]$ . Then, the composition  $(f \circ g)(x) \in \mathbb{Q}[[x]]$  if either  $f$  is a polynomial or  $\text{CF}[x^0, g(x)] = 0$ . Moreover, if  $\text{CF}[x^0, f(x)] = 0$ , then there exists  $g \in \mathbb{Q}[[x]]$ , with  $\text{CF}[x^0, g(x)] = 0$ , such that  $(f \circ g)(x) = x$ . Furthermore,  $(g \circ f)(x) \in \mathbb{Q}[[x]]$  and  $(g \circ f)(x) = x$ .*

*Proof.* As  $(f \circ g)(x) \in \mathbb{Q}[[x]]$ , let  $(f \circ g)(x) = \sum_{k \geq 0} c_k x^k$  and suppose that either  $f$  is a polynomial or  $\text{CF}[x^0, g(x)] = 0$ . Then, to compute  $c_k = \text{CF}[x^k, (f \circ g)(x)]$ , for  $k \geq 0$ , one just needs to consider the terms  $\sum_{n=0}^k a_n (g(x))^n$ , whenever  $f(x) = \sum_{n \geq 0} a_n x^n$ . Hence, each  $c_k \in \mathbb{Q}$  and thus,  $(f \circ g)(x) \in \mathbb{Q}[[x]]$ .

This completes the proof of the first part. We leave the proof of the other part for the reader. ■

The proof of the next result is left for the reader.

**Proposition 3.8. [Basic facts]** *Recall the following statements from Binomial theorem.*

- $\text{CF}[x^n, (1-x)^{-1} = (1+x+x^2+\dots)] = 1$ .

- $(a_0 + a_1 x + \dots)(1+x+x^2+\dots) = a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + \dots$ .

- $\text{CF}[x^n, (1-x)^{-r} = (1+x+x^2+\dots)^r] = C(n+r-1, n)$ . Thus,

$$(1-x)^{-5} = C(4,4) + C(5,4)x + C(6,4)x^2 + \dots$$

- $(1-x^m)^n = 1 - C(n,1)x^m + C(n,2)x^{2m} - \dots + (-1)^n x^{nm}$ .

- $(1+x+x^2+\dots+x^{m-1})^n = \left(\frac{1-x^m}{1-x}\right)^n = (1-x^m)^n (1+x+x^2+\dots)^n$ .

We now define the formal differentiation in  $\mathbb{Q}[[x]]$  and give some important results. The proof is left for the reader.

**Definition 3.9.** Let  $f(x) = \sum_{n \geq 0} a_n x^n \in \mathbb{Q}[[x]]$ .

1. **[Formal Differentiation]** Then, the formal differentiation of  $f(x)$ , denoted  $f'(x)$ , is defined by

$$f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} + \cdots = \sum_{n \geq 1} na_nx^{n-1}.$$

2. **[Formal Integration]** Then, the formal integration of  $f(x)$ , denoted  $\int f(x)$ , is defined by

$$\int f(x)dx = \alpha + a_0x + \frac{a_1}{2}x^2 + \cdots + \frac{a_n}{n+1}x^{n+1} + \cdots = \alpha + \sum_{n \geq 0} \frac{a_n}{n+1}x^{n+1}.$$

**Proposition 3.10. [ogf: tricks]** Let  $g(x), h(x)$  be the ogf's for the sequences  $(a_n), (b_n)$ , respectively. Then, the following are true.

1.  $Ag(x) + Bh(x)$  is the ogf for  $(Aa_n + Bb_n)$ .
2.  $(1-x)g(x)$  is the ogf for the sequence  $a_0, a_1 - a_0, a_2 - a_1, \dots$ .
3.  $(1+x+x^2+\cdots)g(x) = (1-x)^{-1}g(x)$  is the ogf for  $(M_n)$ , where  $M_n = a_n + a_{n-1} + \cdots + a_0$ .
4.  $g(x)h(x)$  is the ogf for  $(c_n)$ , where  $c_n = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \cdots + a_nb_0$ .
5.  $xf'(x)$  is the ogf for  $na_n, n = 1, 2, \dots$ .

**Example 3.11.** 1. Let  $a_r = 1$  for all  $r \geq 0$ . Then, the ogf of the sequence  $(a_r)$  equals  $1 + x + x^2 + \cdots = (1-x)^{-1} = f(x)$ . So, for  $r \geq 0$ , the ogf for

- (a)  $a_r = r$  for all  $r \geq 1$  is  $xf'(x)$  and
- (b)  $a_r = r^2$  for all  $r \geq 1$  is  $x(f'(x) + xf''(x))$ .
- (c) Using the above two examples, the ogf of the sequence  $a_r = 3r + 5r^2$  for all  $r \geq 1$  is  $3xf'(x) + 5(xf'(x) + x^2f''(x)) = 8x(1-x)^{-2} + 10x^2(1-x)^{-3}$ .

2. Determine the number of ways to distribute 50 coins among 30 students so that no student gets more than 4 coins equals

$$\begin{aligned} \text{CF}[x^{50}, (1+x+x^2+x^3+x^4)^{30}] &= \text{CF}[x^{50}, (1-x^5)^{30}(1-x)^{-30}] \\ &= \text{CF}[x^{50}, (1-x^5)^{30} (C(29, 29) + C(30, 29)x + C(31, 29)x^2 + \cdots)] \\ &= C(79, 50) - 30C(74, 45) + C(30, 2)C(69, 40) + \cdots \\ &= \sum_{i=0}^{10} (-1)^i C(30, i)C(79-5i, 29). \end{aligned}$$

3. For  $n, r \in \mathbb{N}$ , determine the number of solutions to  $y_1 + \cdots + y_n = r$  with  $y_i \in \mathbb{N}_0, 1 \leq i \leq n$ .

**Ans:** Recall that this number equals  $C(r+n-1, r)$  (see Theorem 5.3.1).

**Alternate.** We can think of the problem as follows: the above system can be interpreted as coming from the monomial  $x^r$ , where  $r = y_1 + \cdots + y_n$ . Thus, the problem reduces to finding the coefficients of  $x^{y_k}$  of a formal power series, for  $y_k \geq 0$ . Now, recall that  $\text{CF}[x^{y_k}, (1-x)^{-1}] = 1$ . Hence, the question reduces to computing

$$\text{CF}\left[x^r, \frac{1}{(1-x)(1-x)\cdots(1-x)}\right] = \text{CF}\left[x^r, \frac{1}{(1-x)^n}\right] = C(r+n-1, r).$$

4. Evaluate  $S := \sum_{k=0}^{\infty} \frac{k}{2^k} = \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \dots$ .

**Ans:** Note that

$$2S = 1 + \frac{2}{2} + \frac{3}{2^2} + \frac{4}{2^3} + \dots$$

$$S = 0 + \frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \dots$$

$$S = 1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \dots = 2.$$

**Alternate.** Put  $f(x) = (1 - x)^{-1}$ . Then, it has 1 as its radius of convergence and within this radius, the derivative is the same as the power series obtained by term by term differentiation. Thus,  $f'(x) = 1 + 2x + 3x^2 + \dots$  has 1 as its radius of convergence. Hence,

$$S = \frac{1}{2} f'(1/2) = 2.$$

**Alternate.** Alternately (rearranging terms of an absolutely convergent series) it is

$$\begin{array}{r} \frac{1}{2} \qquad \qquad \qquad + \\ \frac{1}{4} + \frac{1}{4} \qquad \qquad \qquad + \\ \frac{1}{8} + \frac{1}{8} + \frac{1}{8} \qquad \qquad \qquad + \\ \vdots \\ \hline 1 + \frac{1}{2} + \dots = 2. \end{array}$$

**EXERCISE 3.12.** 1. Determine a closed form expression for  $\sum_{n \geq 0} nx^n \in \mathbb{Q}[[x]]$ . Or in other words,

write  $\sum_{n \geq 0} nx^n = \frac{p(x)}{q(x)}$ , where  $p(x), q(x)$  are polynomials with integer coefficients.

2. Determine the sum of the first  $N$  positive integers.
3. Determine the sum of the squares of the first  $N$  positive integers.
4. Determine a closed form expression for  $\sum_{n \geq 0} \frac{n^2 + 5n + 16}{n!}$ .
5. Determine a closed form expression for  $\sum_{k=1}^N k^3$ .
6. For  $n, r \in \mathbb{N}$  determine the number of non-negative solutions to  $x_1 + 2x_2 + \dots + nx_n = r$  in the unknowns  $x_i$ 's.
7. Determine  $\sum_{k=0}^{\infty} \frac{1}{2^k} C(n + k - 1, k)$ .
8. Find the number of non-negative integer solutions of  $a + b + c + d + e = 27$ , satisfying
  - (a)  $3 \leq a \leq 8$ ,
  - (b)  $3 \leq a, b, c, d \leq 8$
  - (c)  $c$  is a multiple of 3 and  $e$  is a multiple of 4.
9. Determine the number of ways in which 150 voters can cast their 150 votes for 5 candidates such that no candidate gets more than 30 votes.
10. Verify the following table of formal power series.



Table of Formal Power Series

$e^x = \sum_{k \geq 0} \frac{x^k}{k!}$	$(1+x)^n = \sum_{r \geq 0} C(n, r)x^r, n \in \mathbb{N}_0$
$\cos(x) = \sum_{r \geq 0} \frac{(-1)^r x^{2r}}{(2r)!}$	$\sin(x) = \sum_{r \geq 0} \frac{(-1)^r x^{2r+1}}{(2r+1)!}$
$\cosh(x) = \sum_{r \geq 0} \frac{x^{2r}}{(2r)!}$	$\sinh(x) = \sum_{r \geq 0} \frac{x^{2r+1}}{(2r+1)!}$
Radius of convergence: $ x  < 1$	
$\frac{1}{1-x} = \sum_{k \geq 0} x^k$	$\frac{1}{(1-x)^n} = \sum_{k \geq 0} C(n+k-1, k)x^k, n \in \mathbb{N}$
$\frac{(1+x)^n}{x^r} = \sum_{k \geq -r} C(n, r+k)x^k$	$\frac{x^n}{(1-x)^{n+1}} = \sum_{k \geq 0} C(k, n)x^k, n \in \mathbb{N}_0$
Radius of convergence: $ x  < \frac{1}{4}$	
$\frac{1}{\sqrt{1-4x}} = \sum_{k \geq 0} C(2k, k)x^k$	$\frac{1-\sqrt{1-4x}}{2x} = \sum_{k \geq 0} \frac{1}{k+1} C(2k, k)x^k$

11. Find the ogf of the Fibonacci sequence  $(F_n)_{n \geq 0} := (1, 1, 2, 3, \dots)$ ? Hence, show that for  $n \geq 1$ ,  $F_n$  is the number of ways to write  $n$  as a sum of 1's and 2's.

12. Take a natural number  $n$ . Find

$$C(n, 0)2^n - C(n-1, 1)2^{n-2} + C(n-2, 2)2^{n-4} - C(n-3, 3)2^{n-6} + \dots$$

13. We know  $(1-x)^{-2} = 1 + 2x + 3x^2 + \dots$ . Also,

$$(1-x)^{-2} = (1+x^2-2x)^{-1} = (1-[2x-x^2])^{-1} = 1 + [2x-x^2] + [2x-x^2]^2 + \dots$$

So, can you verify this identity, i.e., the coefficient of  $x_n$  in the later expression is actually  $n+1$ ?

## Generating Functions and Partitions of $n$

Recall from Page 95 that a partition of  $n$  into  $k$  parts is a tuple  $(n_1, \dots, n_k) \in \mathbb{N}^k$  written in non-increasing order, that is,  $n_1 \geq n_2 \geq \dots \geq n_k$ , such that  $n_1 + n_2 + \dots + n_k = n$ . Also, recall that  $\pi_n$  is the number of distinct partitions of  $n$ . The following result due to Euler gives the generating function of  $\pi_n$ .

**Theorem 3.13.** [Euler: partition of  $n$ ] The generating function for  $\pi_n$  is

$$\varepsilon(x) = (1+x+x^2+\dots)(1+x^2+x^4+\dots)\dots(1+x^n+x^{2n}+\dots) = \frac{1}{(1-x)(1-x^2)\dots(1-x^n)}.$$

*Proof.* Note that any partition  $\lambda$  of  $n$  has  $m_1$  copies of 1,  $m_2$  copies of 2 and so on till  $m_n$  copies of  $n$ , where  $m_i \in \mathbb{N}_0$  for  $1 \leq i \leq n$  and  $\sum_{i=1}^n m_i = n$ . Hence,  $\lambda$  uniquely corresponds to  $(x^1)^{m_1}(x^2)^{m_2}\dots(x^n)^{m_n}$  in the word-expansion of

$$(1+x+x^2+\dots)(1+x^2+x^4+\dots)\dots(1+x^n+x^{2n}+\dots).$$

Thus,  $\pi_n = \text{CF}[x^n, \varepsilon(x)]$ . ■

The next result is the same idea as Theorem 6.3.13 and hence the proof is omitted.

**Theorem 3.14.** The number of partitions of  $n$  with entries at most  $r$  is CF

$$\left[ x^n, \prod_{i=1}^r \frac{1}{1-x^i} \right].$$

**Corollary 3.15.** Fix  $n, r \in \mathbb{N}$ . Then, the ogf for the number of partitions of  $n$  into at most  $r$  parts, is  $\frac{1}{(1-x)(1-x^2)\cdots(1-x^r)}$ .

*Proof.* Note that by using Ferrer's diagram (taking conjugate) we see that the number of partitions of  $n$  into at most  $r$  parts is same as the number of partitions of  $n$  with entries at most  $r$ . So, by Theorem 6.3.14, this number is CF  $\left[ x^n, \prod_{i=1}^r \frac{1}{1-x^i} \right]$ . ■

**Theorem 3.16.** [ogf of  $\pi_n(r)$ ] Fix  $n, r \in \mathbb{N}$ . Then, the ogf for  $\pi_n(r)$ , the number of partitions of  $n$  into  $r$  parts, is  $\frac{x^r}{(1-x)(1-x^2)\cdots(1-x^r)}$ .

*Proof.* Consider a partition  $(\lambda_1, \dots, \lambda_r)$  of  $n$ . So,  $n \geq r$ . Assume that  $\lambda_1, \dots, \lambda_k > 1$  and  $\lambda_{k+1}, \dots, \lambda_r = 1$ . Then  $(\lambda_1 - 1, \dots, \lambda_k - 1)$  is a partition of  $n - r$  into at most  $r$  parts.

Conversely, if  $(\mu_1, \dots, \mu_k), k \leq r$ , is a partition of  $n - r$  into at most  $r$  parts, then  $(\mu_1 + 1, \dots, \mu_k + 1, 1, \dots, 1)$ , where the number of 1's is  $r - k$  times, is an  $r$  partition of  $n$ .

Thus, the number of  $r$  partitions of  $n$  is the same as the number of partitions of  $n - r$  with at most  $r$  parts. Thus, by Corollary 6.3.15 the required number is CF  $\left[ x^{n-r}, \frac{1}{(1-x)(1-x^2)\cdots(1-x^r)} \right]$ . Hence, the ogf for  $\pi_n(r)$  is

$$\frac{x^r}{(1-x)(1-x^2)\cdots(1-x^r)}.$$

**EXERCISE 3.17.** 1. For  $n, r \in \mathbb{N}$ , prove that  $\pi_n(r)$  is the number of partitions of  $n + C(r, 2)$  into  $r$  unequal parts.

2. Let  $P, M \subseteq \mathbb{N}$  and  $f(n)$  be the number of partitions of  $n$  where parts are from  $P$  and multiplicities are from  $M$ . Find the generating function for the numbers  $f(n)$ .

**Theorem 3.18.** Suppose there are  $k$  types of objects.

1. If there is an unlimited supply of each object, then the egf of the number of  $r$ -permutations is  $e^{kx}$ .

2. If there are  $m_i$  copies of  $i$ -th object, then the egf of the number of  $r$ -permutations is

$$\left( 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{m_1}}{m_1!} \right) \cdots \left( 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{m_k}}{m_k!} \right).$$

3. Moreover,  $n!S(r, n)$  is the coefficient of  $\frac{x^r}{r!}$  in  $(e^x - 1)^n$ .

*Proof.*

1. Since there are unlimited supply of each object, the egf for each object corresponds to  $e^x = 1 + x + \cdots + \frac{x^n}{n!} + \cdots$ . Hence, the required result follows.

2. Similar to the first part.

3. Recall that  $n!S(r, n)$  is the number of surjections from  $\{1, 2, \dots, r\}$  to  $X = \{s_1, \dots, s_n\}$ . Each surjection can be viewed as a word of length  $r$  of elements of  $X$ , with each  $s_i$  appearing at least once. Thus, we need a selection of  $k_i \in \mathbb{N}$  copies of  $s_i$ , with  $\sum_{i=1}^n k_i = r$ . Also, by Exercise 5.4.7.8, this number equals  $C(r; k_1, \dots, k_n)$ . Hence,

$$n!S(r, n) = r! \text{CF} \left[ x^r, \left( x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \right)^n \right] = \text{CF} \left[ \frac{x^r}{r!}, (e^x - 1)^n \right].$$

**Example 3.19.** 1. In how many ways can you get Rs 2007 using denominations 1, 10, 100, 1000 only?

**Ans:**  $\text{CF} \left[ x^{2007}, \frac{1}{(1-x)(1-x^{10})(1-x^{100})(1-x^{1000})} \right]$ .

2. If we use at most 9 of each denomination in Part 1, then this number is

$$\text{CF} \left[ x^{2007}, \left( \sum_{i=1}^9 x^i \right) \left( \sum_{i=1}^9 x^{10i} \right) \left( \sum_{i=1}^9 x^{100i} \right) \left( \sum_{i=1}^9 x^{1000i} \right) \right] = \text{CF} \left[ x^{2007}, \frac{1-x^{10000}}{1-x} \right] = 1.$$

3. Every natural number has a unique base- $r$  representation ( $r \geq 2$ ). Note that Part 2 corresponds to the case  $r = 10$ .

4. Consider  $n$  integers  $k_1 < k_2 < \dots < k_n$  with  $\gcd(k_1, \dots, k_n) = 1$ . Then, the number of natural numbers not having a partition using  $\{k_1, \dots, k_n\}$  is finite. Determining the largest such integer (**Frobenius number**) is the **coin problem/ money changing problem**. The general problem is NP-hard. No closed form formula is known for  $n > 3$ .

Some times we have a way to obtain a recurrence relation from the generating function. This is important and hence study the next example carefully.

**Example 3.20.** 1. Suppose  $F = \frac{1}{(1-x)(1-x^{10})(1-x^{100})(1-x^{1000})} = \sum_{n \geq 0} a_n x^n$ . Then, taking log and differentiating, we get

$$F' = F \left[ \frac{1}{1-x} + \frac{10x^9}{1-x^{10}} + \frac{100x^{99}}{1-x^{100}} + \frac{1000x^{999}}{1-x^{1000}} \right].$$

So,

$$n a_n = \text{CF} [x^{n-1}, F'] = \text{CF} \left[ x^{n-1}, F \left[ \frac{1}{1-x} + \frac{10x^9}{1-x^{10}} + \frac{100x^{99}}{1-x^{100}} + \frac{1000x^{999}}{1-x^{1000}} \right] \right] = \sum_{k=1}^n a_{n-k} b_k,$$

where

$$b_k = \text{CF} \left[ x^{k-1}, \left[ \frac{1}{1-x} + \frac{10x^9}{1-x^{10}} + \frac{100x^{99}}{1-x^{100}} + \frac{1000x^{999}}{1-x^{1000}} \right] \right] = \begin{cases} 1 & \text{if } 10 \nmid k \\ 11 & \text{if } 10|k, 100 \nmid k \\ 111 & \text{if } 100|k, 1000 \nmid k \\ 1111 & \text{else.} \end{cases}$$

2. We know that  $\lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{k} = \infty$ . What about  $\lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{p_k}$ , where  $p_k$  is the  $k$ -th prime?

**Ans:** For  $n > 1$ , let  $s_n = \sum_{k=1}^n \frac{1}{k}$ . Then, note that

$$s_n \leq \left( 1 + \frac{1}{2} + \frac{1}{4} + \dots \right) \left( 1 + \frac{1}{3} + \frac{1}{9} + \dots \right) \dots \left( 1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \dots \right) = \prod_{k=1}^n \left( 1 + \frac{1}{p_k - 1} \right).$$

Thus,

$$\log s_n \leq \log \left( \prod_{k=1}^n \left( 1 + \frac{1}{p_k - 1} \right) \right) \leq \sum_{k=1}^n \log \left( 1 + \frac{1}{p_k - 1} \right) \leq \sum_{k=1}^n \frac{1}{p_k - 1} \leq 1 + \sum_{k=1}^{n-1} \frac{1}{p_k}.$$

As  $n \rightarrow \infty$ , we see that  $\lim_{n \rightarrow \infty} \sum_{i=1}^n \frac{1}{p_i} = \infty$  as  $\lim_{n \rightarrow \infty} \log s_n = \infty$ .

3. Let  $X$  be the set of natural numbers with only prime divisors 2, 3, 5, 7. Then,

$$1 + \sum_{n \in X} \frac{1}{n} = \left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) \left(1 + \frac{1}{3} + \frac{1}{9} + \dots\right) \dots \left(1 + \frac{1}{7} + \frac{1}{49} + \dots\right) = \frac{2}{1} \frac{3}{2} \frac{5}{4} \frac{7}{6} = \frac{35}{8}.$$

**EXERCISE 3.21.** 1. Let  $\sigma(n) = \sum_{d|n} d$ , for  $n \in \mathbb{N}$ . Then, prove that  $n\pi_n = \sum_{k=1}^n \pi_{n-k} \sigma(k)$ .

2. A Durfee square is the largest square in a Ferrer's diagram. Find the generating function for the number of self conjugate partitions of  $n$  with a fixed size  $k$  of the corresponding Durfee square.

Show that  $(1+x)(1+x^3) \dots = 1 + \sum_{k=1}^{\infty} \frac{x^{k^2}}{(1-x^2)(1-x^4) \dots (1-x^{2k})}$ .

3. Show that the number of partitions of  $n$  into distinct terms is the same as the number of partitions of  $n$  into odd terms.

4. Find the number of  $r$ -digit binary numbers that can be formed using an even number of 0s and an even number of 1s.

5. Find the egf of the number of words of size  $r$  using  $A, B, C, D, E$ ,

(a) if the word has all the letters and the letter  $A$  appears an even many times.

(b) if the word has all the letters and the first letter of the word appears an even number of times.

6. A permutation  $\sigma$  of  $\{1, 2, \dots, n\}$  is said to be **connected** if there does not exist  $k$ ,  $1 \leq k < n$  such that  $\sigma$  takes  $\{1, 2, \dots, k\}$  to itself. Let  $c_n$  denote the number of connected permutations of  $\{1, 2, \dots, n\}$  (convention:  $c_0 = 0$ ), then show that

$$\sum_{k=1}^n c_k (n-k)! = n!.$$

Hence, derive the relationship between the generating functions of  $(n!)$  and  $(c_n)$ .

7. Let  $f(n, r)$  be the number of partitions of  $n$  where each part repeats less than  $r$  times. Let  $g(n, r)$  be the number of partition of  $n$  where no part is divisible by  $r$ . Show that  $f(n, r) = g(n, r)$ .

8. Find the number of 9-sequences that can be formed using 0, 1, 2, 3 in each case:

(a) The sequence has an even number of 0s.

(b) The sequence has an odd number of 1s and an even number of 0s.

(c) No digit appears exactly twice.

## Recurrence Relation

**Definition 4.1.** [Recurrence Relation] A **recurrence relation** is a way of recursively defining the terms of a sequence as a function of preceding terms together with certain initial conditions.

**Example 4.2.**  $a_n = 3 + 2a_{n-1}$  for  $n \geq 1$  with the **initial condition**  $a_0 = 1$  is a recurrence relation. Note that it completely determines the sequence  $(a_n) = \{1, 5, 13, 29, 61, \dots\}$ .

**Definition 4.3.** [Difference Equation] For a sequence  $(a_n)$ , the **first difference**  $d(a_n)$  is  $a_n - a_{n-1}$ . The  **$k$ -th difference**  $d_k(a_n) = d_{k-1}(a_n) - d_{k-1}(a_{n-1})$ . A **difference equation** is an equation involving  $a_n$  and its differences.

**Example 4.4.** 1.  $a_n - d^2(a_n) = 5$  is a difference equation. But, note that it doesn't give a recurrence relation as we don't have any initial condition(s).

2. Every recurrence relation can be expressed as a difference equation. The difference equation corresponding to the recurrence relation  $a_n = 3 + 2a_{n-1}$  is  $a_n = 3 + 2(a_n - d(a_n))$ .

**Definition 4.5. [Solution of a Recurrence Relation]** A **solution** of a recurrence relation is a function  $u(n)$ , generally denoted by  $u_n$ , satisfying the recurrence relation.

**Example 4.6.** 1.  $u(n) = 2^{n+2} - 3$  is a solution of  $a_n = 3 + 2a_{n-1}$  with  $a_0 = 1$ .

2. The **Fibonacci sequence** is given by  $a_n = a_{n-1} + a_{n-2}$  for  $n \geq 2$  with  $a_0 = 0$ ,  $a_1 = 1$ . Use  $\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2}$  and  $\left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{3-\sqrt{5}}{2}$  to verify that  $a_n = \frac{1}{\sqrt{5}} \left( \left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right)$  is a solution of the recurrence relation that defines the Fibonacci sequence.

**Definition 4.7. [LNRC/LHRC]** A recurrence relation is called a **linear nonhomogeneous recurrence relation** with constant coefficients (**LNRC**) of order  $r$  if, for a known function  $f$

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + f(n), \text{ where } c_i \in \mathbb{R} \text{ for } 1 \leq i \leq r, c_r \neq 0. \quad (6.3)$$

If  $f = 0$ , then Equation (6.3) is homogeneous and is called the associated **linear homogeneous recurrence relation** with constant coefficients (**LHRC**).

**Theorem 4.8.** For  $k \in \mathbb{N}$  and  $1 \leq i \leq k$ , let  $f_i$  be known functions. Consider the  $k$  number of LNRC

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + f_i(n) \text{ for } i = 1, \dots, k, \quad (6.4)$$

with the same set of initial conditions. If  $u_i(n)$  is a solution of the  $i$ -th recurrence relation, then

$$a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r} + \sum_{i=1}^k \alpha_i f_i(n) \quad (6.5)$$

with the same set of initial conditions has  $\sum_{i=1}^k \alpha_i u_i(n)$  as its solution.

*Proof.* The proof is left as an exercise for the reader.

**Definition 4.9. [Characteristic Equation]** The equation  $x^r - c_1 x^{r-1} - \cdots - c_r = 0$  is called the **characteristic equation** of the LHRC  $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$  with  $c_r \neq 0$ . The roots of the characteristic equation are called the **characteristic roots** of the LHRC.

Observe that if  $a_n = x^n$  is a solution of the LHRC  $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$  with  $c_r \neq 0$ , then either  $x = 0$  or  $x$  is a characteristic root. Further, if  $x_1, \dots, x_r$  are the characteristic roots, then  $a_n = x_i^n$  is a solution of the LHRC. It follows that  $a_n = \sum_{i=1}^r \alpha_i x_i^n$  for  $\alpha_i \in \mathbb{R}$  is a solution of the given LHRC. We show that the latter form of a solution is a general solution so that a given set of initial conditions may be satisfied.

**Theorem 4.10. [General Solution: Distinct Roots]** If the characteristic roots  $x_1, \dots, x_r$  of an LHRC are distinct, then every solution of the LHRC is a linear combination of  $x_1^n, \dots, x_r^n$ . Moreover, the solution is unique if  $r$  consecutive initial conditions are given.

*Proof.* Let  $u(n)$  be any solution of a given LHRC  $a_n = c_1 a_{n-1} + \cdots + c_r a_{n-r}$ . That is,

$$u(n) = \sum_{j=1}^r c_j u(n-j) = c_1 u(n-1) + \cdots + c_r u(n-r).$$

We show that there exist  $\alpha_1, \dots, \alpha_r \in \mathbb{R}$  such that  $u(n) = \sum_{i=1}^r \alpha_i x_i^n$  for all  $n \in \mathbb{W}$ . We first consider a smaller problem, that is, whether the first  $r$  values of  $u(n)$  can be expressed in this form. The answer will be affirmative provided we can determine the constants  $\alpha_1, \dots, \alpha_r$  so that  $u(n) = \sum_{i=1}^r \alpha_i x_i^n$  for  $n = 0, 1, \dots, r - 1$ . To explore this, substitute  $n = 0, 1, \dots, r - 1$  to obtain the following linear system in the unknowns  $\alpha_1, \dots, \alpha_r$ :

$$\begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(r-1) \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_r \\ & \ddots & \\ x_1^{r-1} & \cdots & x_r^{r-1} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_r \end{bmatrix}.$$

Since the above  $r \times r$  matrix (commonly known as the Vandermonde matrix) is invertible, there exist  $\alpha_1, \dots, \alpha_r$  such that  $u(n) = \sum_{i=1}^r \alpha_i x_i^n$  for  $0 \leq n \leq r - 1$ . Hence, we have proved the result for the first  $r$  values of  $u(n)$ . So, let us assume that  $u(n) = \sum_{i=1}^r \alpha_i x_i^n$  for  $0 \leq n < k$ , where  $k \geq r$ . Notice that for  $n = k$ ,  $x_i^k$  is a solution of the given LHRC. So,  $x_i^k = \sum_{j=1}^r c_j x_i^{k-j}$ . Then

$$u(k) = \sum_{j=1}^r c_j u(k-j) = \sum_{j=1}^r c_j \sum_{i=1}^r \alpha_i x_i^{k-j} = \sum_{i=1}^r \alpha_i \sum_{j=1}^r c_j x_i^{k-j} = \sum_{i=1}^r \alpha_i x_i^k.$$

Hence by PMI,  $u(n) = \sum_{i=1}^r \alpha_i x_i^n$  for all  $n$ .

For uniqueness, suppose  $u(n)$  and  $v(n)$  are solutions of the LHRC satisfying the  $r$  initial conditions  $u(i) = v(i) = a_i$  for  $0 \leq i \leq r - 1$ . Write  $y(n) = u(n) - v(n)$ . Then  $y(n)$  satisfies the same LHRC with initial conditions  $y(0) = \dots = y(r-1) = 0$ . By what we have just proved,  $y(n) = \sum_{i=1}^r \gamma_i x_i^n$  for some constants  $\gamma_1, \dots, \gamma_r$ . Treating  $\gamma_i$ s as unknowns, and substituting  $n = 0, 1, \dots, r - 1$ , we arrive at a linear system as above, where  $u$  is replaced by  $y$ . Since the system matrix there is invertible, it leads to the unique solution  $\gamma_1 = \dots = \gamma_r = 0$ . In turn, we obtain  $y(n) = 0$  for all  $n$ . That is,  $u(n) = v(n)$  for all  $n$ . ■

Notice that the characteristic roots are, in general, complex numbers, so that the constants in the linear combination can be complex numbers.

**Example 4.11.1.** Solve  $a_n - 4a_{n-2} = 0$  for  $n \geq 2$  with  $a_0 = 1$  and  $a_1 = 1$ . **Ans:** The characteristic equation is  $x^2 - 4 = 0$ . As the characteristic roots  $x = \pm 2$  are distinct, the general solution is  $a_n = \alpha(-2)^n + \beta 2^n$ . The initial conditions give  $\alpha + \beta = 1$  and  $2\beta - 2\alpha = 1$ . Hence,  $\alpha = \frac{1}{4}, \beta = \frac{3}{4}$ . Thus, the unique solutions is  $a_n = 2^{n-2}(3 + (-1)^n)$ .

2. Solve  $a_n = 3a_{n-1} + 4a_{n-2}$  for  $n \geq 2$  with  $a_0 = 1$  and  $a_1 = c$ , a constant. **Ans:** The characteristic equation is  $x^2 - 3x - 4 = 0$ . The characteristic roots are  $-1$  and  $4$ ; they are distinct. The general solution is  $a_n = \alpha(-1)^n + \beta 4^n$ . The initial conditions imply  $\alpha = \frac{4-c}{5}$  and  $\beta = \frac{1+c}{5}$ . Thus, the unique general solution is  $a_n = \frac{1}{5}((4-c)(-1)^n + (1+c)4^n)$ .

3. Solve the Fibonacci recurrence  $a_n = a_{n-1} + a_{n-2}$  with initial conditions  $a_0 = 0, a_1 = 1$ . **Ans:** The characteristic equation  $x^2 - x - 1 = 0$  gives distinct characteristic roots as  $\frac{1 \pm \sqrt{5}}{2}$ . So, the general solution is  $a_n = \alpha \left(\frac{1+\sqrt{5}}{2}\right)^n + \beta \left(\frac{1-\sqrt{5}}{2}\right)^n$ . Using the initial conditions, we get  $\alpha = 1/\sqrt{5}, \beta = -\alpha = -1/\sqrt{5}$ . Hence, the required solution is

$$a_n = \frac{1}{\sqrt{5}} \left[ \left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right].$$

4. Solve the recurrence relation  $a_n + a_{n-2} = 0$  with the initial conditions  $a_0 = a_1 = 2$ . **Ans:** The characteristic equation is  $x^2 + 1 = 0$  with distinct characteristic roots as  $\pm i$ . The general solution is in the form  $a_n = \alpha i^n + \beta (-i)^n$ . Initial conditions imply that  $\alpha + \beta = 2$  and  $\alpha i - \beta i = 2$ . So,  $\alpha = 1 - i$  and  $\beta = 1 + i$ . Then  $a_n = (1 - i)i^n + (1 + i)(-i)^n$ .
5. Consider a triangle with vertices  $(a_1, b_1) = (0, 0)$ ,  $(a_2, b_2) = (5, 0)$  and  $(a_3, b_3) = (3, 7)$ . For  $n > 3$ , define  $(a_n, b_n)$  as the centroid of the triangle formed by  $(a_{n-1}, b_{n-1})$ ,  $(a_{n-2}, b_{n-2})$  and  $(a_{n-3}, b_{n-3})$ . Does the sequence  $((a_n, b_n))$  converge? If so, to what limit?

**Ans:** Note that the sequence  $((a_n, b_n))$  converges if and only if both the sequences  $(a_n)$  and  $(b_n)$  converge. We will first show that  $(a_n)$  converges.

Let  $M_1 = \max\{a_1, a_2, a_3\}$  and  $m_1 = \min\{a_1, a_2, a_3\}$ . Notice that  $m_1 \leq a_1, a_2, a_3 \leq M_1$ . Hence,

$$\begin{aligned} m_1 &\leq \frac{a_1 + a_2 + a_3}{3} \leq \frac{2M_1 + m_1}{3}, \text{ i.e., } m_1 \leq a_4 \leq \frac{2M_1 + m_1}{3}; \\ m_1 &\leq \frac{a_2 + a_3 + a_4}{3} \leq \frac{2M_1 + a_4}{3} \leq \frac{8M_1 + m_1}{9}, \text{ i.e., } m_1 \leq a_5 \leq \frac{8M_1 + m_1}{9}; \quad \text{and} \\ m_1 &\leq \frac{a_3 + a_4 + a_5}{3} \leq \frac{26M_1 + m_1}{27}, \text{ i.e., } m_1 \leq a_6 \leq \frac{26M_1 + m_1}{27}. \end{aligned}$$

As  $\frac{2M_1 + m_1}{3} \leq \frac{8M_1 + m_1}{9} \leq \frac{26M_1 + m_1}{27}$ , we see that

$$m_1 \leq a_4, a_5, a_6 \leq \frac{26M_1 + m_1}{27}.$$

Let  $M_2 = \max\{a_4, a_5, a_6\}$  and  $m_2 = \min\{a_4, a_5, a_6\}$ . Then

$$[m_2, M_2] \subseteq [m_1, M_1] \quad \text{and} \quad \text{length}([m_2, M_2]) \leq \frac{26}{27} \text{length}([m_1, M_1]).$$

Similarly, taking  $M_n = \max\{a_{3n+1}, a_{3n+2}, a_{3n+3}\}$  and  $m_n = \min\{a_{3n+1}, a_{3n+2}, a_{3n+3}\}$ , we get a nested sequence of nonempty closed intervals

$$[m_1, M_1] \supseteq [m_2, M_2] \supseteq [m_3, M_3] \supseteq \dots$$

with diameters going to zero. By nested interval theorem,  $\bigcap_{i=1}^{\infty} [m_i, M_i]$  is a singleton set, say,  $\{l\}$ .

Note that,  $[m_{n+1}, M_{n+1}]$  contains all the terms  $a_{3n+1}, a_{3n+2}, a_{3n+3}, a_{3n+4}, \dots$ . It now follows that  $\lim_{n \rightarrow \infty} a_n = l$ . Thus,  $\lim_{n \rightarrow \infty} \frac{a_{n+1} + 2a_{n+2} + 3a_{n+3}}{6} = l$ . But notice that,

$$\frac{a_1 + 2a_2 + 3a_3}{6} = \frac{a_2 + 2a_3 + 3a_4}{6} = \frac{a_3 + 2a_4 + 3a_5}{6} = \dots$$

Thus  $l = \frac{a_1 + 2a_2 + 3a_3}{6}$ . Thus, the limit to the original question is  $(19/6, 7/2)$ .

\* How did we guess the formula? To see that write

$$3a_4 = a_1 + a_2 + a_3$$

$$3a_5 = a_2 + a_3 + a_4$$

$$\vdots$$

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

---


$$3(a_4 + a_5 + \dots + a_{n+3}) = a_1 + 2a_2 + 3(a_3 + \dots + a_n) + 2a_{n+1} + a_{n+2}$$

Cancelling, we get  $a_{n+1} + 2a_{n+2} + 3a_{n+3} = a_1 + 2a_2 + 3a_3$ , which is what we required.

**Alternate.** This method is of interest to us. Note that we have the LHRC

$$a_n = \frac{a_{n-1} + a_{n-2} + a_{n-3}}{3}, \quad n > 3.$$

So, the characteristic equation is  $3x^3 - x^2 - x - 1 = 0$ . Observe that 1 is a root. We now see that  $3x^3 - x^2 - x - 1 = (x - 1)(3x^2 + 2x + 1)$  and so the other two roots are

$$\alpha := \frac{-2 + \sqrt{4 - 12}}{6} = \frac{-1 + i\sqrt{2}}{3} \quad \text{and} \quad \beta := \frac{-1 - i\sqrt{2}}{3}.$$

Hence, by Theorem 6.4.10, there exist constants  $a, b, c \in \mathbb{C}$  such that

$$a_n = a(1)^{n-1} + b(\alpha)^{n-1} + c(\beta)^{n-1}.$$

As  $|\alpha| = |\beta| = \frac{1}{\sqrt{3}} < 1$ , we see that  $a_n \rightarrow a$ . Using the initial conditions, we get

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \alpha & \beta \\ 1 & \alpha^2 & \beta^2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}.$$

Solving for  $a$  gives  $a = \frac{a_1 + 2a_2 + 3a_3}{6}$ .

**Theorem 4.12. [General Solution: Multiple Roots]** *Given an LHRC, let  $t$  be a characteristic root of multiplicity  $s$ . Then  $u(n) = t^n \left( \sum_{i=0}^{s-1} \alpha_i n^i \right)$  is a solution (called a **basic solution**). Moreover, if  $t_1, \dots, t_k$  are the distinct characteristic roots with multiplicities  $s_1, \dots, s_k$ , respectively, then every solution is a sum of the  $k$  corresponding basic solutions.*

*Proof.* It is given that  $t$  is a zero of the polynomial  $F = x^r - c_1 x^{r-1} - \dots - c_r$  of multiplicity  $s$ . Put

$$\begin{aligned} G_0 &= x^{n-r} F = x^n - c_1 x^{n-1} - \dots - c_r x^{n-r} \\ G_1 &= x G'_0 = n x^n - c_1 (n-1) x^{n-1} - \dots - c_r (n-r) x^{n-r} \\ G_2 &= x G'_1 = n^2 x^n - c_1 (n-1)^2 x^{n-1} - \dots - c_r (n-r)^2 x^{n-r} \\ &\vdots \\ G_{s-1} &= x G'_{s-2} = n^{s-1} x^n - c_1 (n-1)^{s-1} x^{n-1} - \dots - c_r (n-r)^{s-1} x^{n-r} \end{aligned}$$

Note that each of  $G_0, G_1, \dots, G_{s-1}$  has a zero at  $t$ , i.e., for  $i = 0, 1, \dots, s-1$ , we have

$$G_i(t) = t^n n^i - c_1 t^{n-1} (n-1)^i - \dots - c_r t^{n-r} (n-r)^i = 0.$$

Thus, for any choice of  $\alpha_i \in \mathbb{R}, 0 \leq i \leq s-1$ , if one defines  $P(k) = \sum_{i=1}^{s-1} k^i \alpha_i$ , for  $k \geq 0$  then

$$0 = \sum_{i=0}^{s-1} \alpha_i G_i(t) = t^n P(n) - c_1 t^{n-1} P(n-1) - \dots - c_r t^{n-r} P(n-r).$$

Hence, by definition  $u(n) - c_1 u(n-1) - \dots - c_r u(n-r) = 0$ . Therefore,  $u(n)$  is a solution of the LHRC.

Now, the second statement follows from Theorem 6.4.10. ■

**Example 4.13.** Suppose that an LHRC has roots 2, 2, 3, 3, 3. Then, the general solution is given by  $2^n(\alpha_1 + n\alpha_2) + 3^n(\beta_1 + n\beta_2 + n^2\beta_3)$ .

Consider the LNRC in Equation (6.3). If  $v_n$  and  $w_n$  are solutions of the LNRC, then  $u_n := w_n - v_n$  satisfies the associated LHRC. That is,  $w_n = u_n + v_n$  shows that any solution  $w_n$  can be expressed as a solution of the associated LHRC plus a solution  $v_n$  of the LNRC. We summarize this finding in the next theorem.



**Theorem 4.14. [LNRC]** Consider the LNRC in Equation (6.3). Let  $u_n$  be a general solution of the associated LHRC. If  $v_n$  is a (particular) solution of the LNRC, then  $a_n = u_n + v_n$  is a general solution of the LNRC.

**Remark 4.15.** Theorem 6.4.14 implies that in order to obtain a general solution of an LNRC, we need to solve the associated LHRC for a general solution and also obtain a particular solution of the same LNRC. Unlike an LHRC, no general algorithm is available to obtain a particular solution of an LNRC. In some cases, heuristic methods can be used to obtain a particular solution. If  $f(n) = a^n$  or  $n^k$  or a linear combination of these, then a particular solution can be easily obtained.

#### Obtaining particular solution after knowledge of the characteristic roots.

1. If  $f(n) = a^n$  and  $a$  is not a root of LHRC, then  $v(n) = ca^n$ .
2. If  $f(n) = a^n$  and  $a$  is a root of LHRC of multiplicity  $t$ , then  $v(n) = cn^t a^n$ .
3. If  $f(n) = n^k$  and 1 is not a root of LHRC, then use  $v(n) = c_0 + c_1 n + \cdots + c_k n^k$ .
4. If  $f(n) = n^k$  and 1 is a root of LHRC of multiplicity  $t$ , then  $v(n) = n^t(c_0 + c_1 n + \cdots + c_k n^k)$ .

**Example 4.16.** 1. Solve  $a_n = 3a_{n-1} + 2n$  for  $n \geq 1$  with  $a_0 = 1$ .

**Ans:** Observe that 3 is the characteristic root of the associated LHRC ( $a_n = 3a_{n-1}$ ). Thus, the general solution of LHRC is  $u_n = 3^n \alpha$ . Note that 1 is not a characteristic root and hence a particular solution is  $a + nb$ , where  $a$  and  $b$  are to be computed using  $a + nb = 3(a + (n-1)b) + 2n$ . This gives  $a = -3/2$  and  $b = -1$ . Hence,  $a_n = 3^n \alpha - n - 3/2$ . Using  $a_0 = 1$ , check that  $\alpha = 5/2$ .

2. Solve  $a_n = 3a_{n-1} - 2a_{n-2} + 3(5)^n$  for  $n \geq 3$  with  $a_1 = 1, a_2 = 2$ .

**Ans:** The associated LHRC ( $a_n = 3a_{n-1} - 2a_{n-2}$ ) has the characteristic roots 1 and 2. Thus, the general solution of the LHRC is  $u_n = \alpha 1^n + \beta 2^n$ . Notice that 5 is not a characteristic root. So,  $v_n = c 5^n$  is a particular solution of LNRC. That is,  $c 5^n = 3c 5^{n-1} - 2c 5^{n-2} + 3(5)^n$ . It gives  $c = 25/4$ . Hence, the general solution of LNRC is in the form  $a_n = \alpha + \beta 2^n + (25/4)5^n$ . One can then determine  $\alpha$  and  $\beta$  from the initial conditions.

3. In the previous example, take  $f(n) = 3(2^n)$ . Trying  $c(2)^n$  as a particular solution, we have  $4c = 6c - 2c + 12$ . This is absurd. The reason is that 2 is a characteristic root of the associated LHRC. Now, with the choice of  $cn(2)^n$  as a particular solution, we get  $4nc = 6(n-1)c - 2(n-2)c + 12$ . It gives  $c = 6$ . Hence, the general solution of LNRC is in the form  $a_n = \alpha + \beta 2^n + 6n2^n$  from which the constants  $\alpha$  and  $\beta$  can be computed using the initial conditions.

## Generating Function from Recurrence Relation

Sometimes we can find a solution to the recurrence relation using the generating function of  $a_n$ ; see the following example.

**Example 5.1.** 1. Consider solving  $a_n = 2a_{n-1} + 1, a_0 = 1$ .

**Ans:** Let  $F(x) = a_0 + a_1 x + \cdots$  be the generating function for  $\{a_i\}$ . Then,

$$F = 1 + \sum_{i=1}^{\infty} a_i x^i = 1 + \sum_{i=1}^{\infty} (2a_{i-1} + 1) x^i = \sum_{i=0}^{\infty} x^i + 2x \sum_{i=0}^{\infty} a_i x^i = \frac{1}{1-x} + 2xF.$$

Hence,  $F(x) = \frac{1}{(1-x)(1-2x)} = \frac{2}{1-2x} - \frac{1}{1-x}$  so that  $a_n = \text{CF}[x^n, F(x)] = 2^{n+1} - 1$ .

2. Find the ogf  $F$  for the Fibonacci recurrence relation  $a_n = a_{n-1} + a_{n-2}$ ,  $a_0 = 0, a_1 = 1$ .

**Ans:** Define  $F(x) = \sum_{n \geq 0} a_n x^n = \sum_{n \geq 1} a_n x^n$ . Then using the recurrence relation, we have

$$F(x) = \sum_{n \geq 0} a_n x^n = x + \sum_{n \geq 2} (a_{n-1} + a_{n-2}) x^n = x + (x + x^2)F(x).$$

So,  $F(x) = \frac{x}{1 - x - x^2}$ .

Let  $\alpha = \frac{1+\sqrt{5}}{2}$  and  $\beta = \frac{1-\sqrt{5}}{2}$ . Verify that  $(1 - \alpha x)(1 - \beta x) = 1 - x - x^2$ . Then

$$F(x) = \frac{1}{\sqrt{5}} \left( \frac{1}{1 - \alpha x} - \frac{1}{1 - \beta x} \right) = \frac{1}{\sqrt{5}} \left( \sum_{n \geq 0} \alpha^n x^n - \sum_{n \geq 0} \beta^n x^n \right).$$

Therefore,  $a_n = \text{CF}[x^n, F(x)] = \frac{1}{\sqrt{5}} \sum_{n \geq 0} (\alpha^n - \beta^n)$ , which equals Equation (6.6).

The next result follows using a small calculation and hence the proof is left for the reader.

**Theorem 5.2. [Obtaining Generating Function from Recurrence Relation]** *Let  $a_n$  be the solution of the  $r$ -th order LHRC with  $r$  initial conditions given by*

$$a_n = c_1 a_{n-1} + \dots + c_r a_{n-r} \quad \text{with } a_0 = A_0, a_1 = A_1, a_{r-1} = A_{r-1}. \tag{6.7}$$

Then the generating function of  $(a_n)$  is obtained by taking

$$\begin{aligned} F(x) &= A_0 + A_1 x + \dots + A_{r-1} x^{r-1} + [(c_1 A_{r-1} + \dots + c_r A_0) x^r + \dots \\ &= A_0 + A_1 x + \dots + A_{r-1} x^{r-1} + c_r x^r F + c_{r-1} x^{r-1} (F(x) - A_0) + \dots + \\ &\quad c_1 x (F(x) - A_0 - A_1 x - \dots - A_{r-2} x^{r-2}). \end{aligned}$$

This implies that

$$F(x) = \frac{\sum_{i=0}^{r-1} A_i x^i - c_1 x \sum_{i=0}^{r-2} A_i x^i - c_2 x^2 \sum_{i=0}^{r-3} A_i x^i - \dots - c_{r-1} x^{r-1} A_0}{1 - c_1 x - \dots - c_r x^r}. \tag{6.8}$$

**Remark 5.3.** Then we observe the following about Equation (6.8) in Theorem 6.5.2.

1. Note that the numerator is a polynomial in  $x$  of degree at most  $r - 1$ , determined by the initial conditions and the denominator  $Q(x)$  is a polynomial of degree  $r$  determined by the recurrence relation.
2. Now consider all solutions of the LHRCC  $a_n = c_1 a_{n-1} + \dots + c_r a_{n-r}$  of order  $r$ . We already know that they form a vector space of dimension  $r$ . Each such solution will give us an ogf as shown above. Since they have the same denominator, if we take linearly independent solutions, we will get linearly independent numerators. It now follows that, if  $P(x)$  has degree less than  $r$ , then  $\frac{P(x)}{Q(x)}$  is an ogf for some solution.
3. Note that we can write  $1 - c_1 x - \dots - c_r x^r = (1 - \alpha_1 x)^{s_1} \dots (1 - \alpha_k x^k)^{s_k}$ , where  $\alpha_i$ 's are distinct complex numbers and  $s_1 + \dots + s_k = r$ . Let  $P_1(x)$  have degree less than  $s_1$ . Then notice that

$$\frac{P_1(x)}{(1 - \alpha_1 x)^{s_1}} = \frac{P_1(x)(1 - \alpha_2 x)^{s_2} \dots (1 - \alpha_k x)^{s_k}}{(1 - \alpha_1 x)^{s_1} (1 - \alpha_2 x)^{s_2} \dots (1 - \alpha_k x)^{s_k}}$$

is an ogf for some solution. Similarly,  $\frac{P_1(x)}{(1-\alpha_1x)^{s_1}}, \dots, \frac{P_k(x)}{(1-\alpha_kx)^{s_1}}$  are ogf's of some solutions. Are these solutions linearly independent? Yes. Indeed, if those solutions are linearly dependent, then a linear combination

$$a_1 \frac{P_1(x)}{(1-\alpha_1x)^{s_1}} + \dots + a_k \frac{P_k(x)}{(1-\alpha_kx)^{s_1}} = 0.$$

But this is not possible, otherwise, multiplying by  $(1-\alpha_1x)^{s_1}(1-\alpha_2x)^{s_2} \dots (1-\alpha_kx)^{s_k}$ , we get  $a_1R_1(x) + \dots + a_kR_k(x)$  is the zero polynomial. As every term except the first one is divisible by  $(1-\alpha_1x)^{s_1}$  and the rhs is also divisible by  $(1-\alpha_1x)^{s_1}$ , and that  $P_1$  has degree less than  $s_1$ , it follows that  $a_1 = 0$ . Similarly, all other  $a_i$  are 0. Thus we already know that the sequences  $(\alpha_1^n), (n\alpha_1^n), \dots, (n^{s_1-1}\alpha_1^n)$  are linearly independent. Indeed, if there is a combination

$$a_0(\alpha_1^n) + a_1(n\alpha_1^n) + \dots + a_{s_1-1}(n^{s_1-1}\alpha_1^n) = (0, 0, \dots),$$

as  $\alpha_1 \neq 0$ , we would get

$$(a_0 + a_1n + a_2n^2 + \dots + a_{s_1-1}n^{s_1-1}) = (0, 0, \dots),$$

implying  $a_0 = a_1 = \dots = a_{s_1-1} = 0$ .

4. Now suppose that, the sequences

$$(\alpha_1^n), (n\alpha_1^n), \dots, (n^{s_1-1}\alpha_1^n), \dots, (\alpha_k^n), (n\alpha_k^n), \dots, (n^{s_k-1}\alpha_k^n)$$

are linearly dependent. We then have

$$(P_1(n)\alpha_1^n + P_2(n)\alpha_2^n + \dots + P_k(n)\alpha_k^n) = (0, 0, \dots),$$

for some polynomials  $P_i(n)$  with degrees less than  $s_i$ ,  $i = 1, \dots, k$ .

We explain Theorem 6.5.2 by considering the following examples.

**Example 5.4.** 1. Find the ogf for the Catalan numbers  $C_n$ 's.

**Ans:** Let  $g(x) = 1 + \sum_{n \geq 1} C_n x^n$ , where  $C_n = \frac{C(2n, n)}{n+1} = \frac{2(2n-1)}{n+1} C_{n-1}$  with  $C_0 = 1$ . Then,

$$\begin{aligned} g(x) - 1 &= \sum_{n \geq 1} C_n x^n = \sum_{n \geq 1} \frac{2(2n-1)}{n+1} C_{n-1} x^n \\ &= \sum_{n=1}^{\infty} \frac{4n+4}{n+1} C_{n-1} x^n + \sum_{n=1}^{\infty} \frac{-6}{n+1} C_{n-1} x^n = 4xg(x) + \frac{-6}{x} \int_0^x tg(t)dt. \end{aligned}$$

So,  $[g(x) - 1 - 4xg(x)]x = -6 \int_0^x tg(t)dt$ . So,  $[g(x) - 1 - 4xg(x)]x = -6 \int_0^x tg(t)dt$ . Differentiate with respect to  $x$  to get

$$x(1-4x)g' + (1-2x)g = 1.$$

It is a linear ordinary differential equation. Observe that

$$\int \frac{1-2x}{x(1-4x)} dx = \int \left[ \frac{1}{x} + \frac{2}{1-4x} \right] dx = \ln \left( \frac{x}{\sqrt{1-4x}} \right).$$

We thus multiply the equation with its integrating factor  $\frac{x}{\sqrt{1-4x}}$  to obtain

$$g(x)' \frac{x}{\sqrt{1-4x}} + g(x) \frac{1-2x}{(1-4x)^{3/2}} = \frac{1}{(1-4x)^{3/2}} \Leftrightarrow \frac{d}{dx} \left[ g(x) \frac{x}{\sqrt{1-4x}} \right] = \frac{1}{(1-4x)^{3/2}}.$$

Hence,  $g(x) \frac{x}{\sqrt{1-4x}} = \frac{1}{2\sqrt{1-4x}} + C$ , where  $C \in \mathbb{R}$ . Or, equivalently  $2xg(x) = 1 + 2C\sqrt{1-4x}$ .

Note that  $C = -\frac{1}{2}$  as  $C_0 = \lim_{x \rightarrow 0} g(x) = 1$ . Therefore, the ogf of the Catalan numbers is

$$g(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

**Alternate.** Recall that  $C_n$  is the number of representations of the product of  $n + 1$  square matrices of the same size, using  $n$  pairs of brackets. From such a representation, remove the leftmost and the rightmost brackets to obtain the product of two representations of the form:

$$A_1(A_2 \cdots A_{n+1}), (A_1 A_2)(A_3 \cdots A_{n+1}), \dots, (A_1 \cdots A_k)(A_{k+1} \cdots A_{n+1}), \dots, (A_1 \cdots A_n)A_{n+1}.$$

Hence, we see that

$$C_n = C_0 C_{n-1} + C_1 C_{n-2} + \dots + C_{n-1} C_0. \tag{6.9}$$

Let  $g(x)$  be the generating function of  $C_n$ ; that is,  $g(x) = \sum_{n=0}^{\infty} C_n x^n$ . Then, for  $n \geq 1$ ,

$$\text{CF}[x^{n-1}, g(x)^2] = \text{CF}\left[x^{n-1}, \left(\sum_{n=0}^{\infty} C_n x^n\right)^2\right] = \sum_{i=0}^{n-1} C_i C_{n-1-i} = C_n \text{ using Equation (6.9)}.$$

That is,  $\text{CF}[x^n, xg(x)^2] = C_n$ . Hence,  $g(x) = 1 + xg(x)^2$ . Solving for  $g(x)$ , we get

$$g(x) = \frac{1}{2} \left( \frac{1}{x} \pm \sqrt{\frac{1}{x^2} - \frac{4}{x}} \right) = \frac{1 \pm \sqrt{1 - 4x}}{2x}.$$

As the function  $g$  is continuous (being a power series in the domain of convergence) and  $\lim_{x \rightarrow 0} g(x) = C_0 = 1$ , it follows that

$$g(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

2. Fix  $r \in \mathbb{N}$  and let  $(a_n)$  be a sequence with  $a_0 = 1$  and  $\sum_{k=0}^n a_k a_{n-k} = C(n+r, r)$  for all  $n \geq 1$ . Determine  $a_n$ .

Answer: Let  $g(x) = \sum_{n \geq 0} a_n x^n$ . Using  $C(n+r, r) = C(n+(r+1)-1, n)$ , we obtain

$$g(x)^2 = \sum_{n \geq 0} \left( \sum_{k=0}^n a_k a_{n-k} \right) x^n = \sum_{n \geq 0} C(n+r, r) x^n = \sum_{n \geq 0} C(n+r, n) x^n = \frac{1}{(1-x)^{r+1}}.$$

Hence,  $a_n = \text{CF}\left[x^n, \frac{1}{(1-x)^{(r+1)/2}}\right]$ . For example, when  $r = 2$

$$a_n = (-1)^n C(-3/2, n) = \frac{3 \cdot 5 \cdot 7 \cdots (2n+1)}{2^n n!} = \frac{(2n+1)!}{2^{2n} n! n!}.$$

3. Determine the sequence  $\{f(n, m) : n, m \in \mathbb{W}\}$  which satisfies  $f(n, 0) = 1$  for all  $n \geq 0$ ,  $f(0, m) = 0$  for all  $m > 0$ , and

$$f(n, m) = f(n-1, m) + f(n-1, m-1) \text{ for } n > 0, m > 0. \tag{6.10}$$

Answer: For  $n > 0$ , define  $F_n(x) = \sum_{m \geq 0} f(n, m)x^m = 1 + \sum_{m \geq 1} f(n, m)x^m$ . Then  $F_1(x) = 1 + x$ , and for  $n \geq 2$ ,

$$\begin{aligned} F_n(x) &= \sum_{m \geq 0} f(n, m)x^m = 1 + \sum_{m \geq 1} (f(n-1, m) + f(n-1, m-1))x^m \\ &= 1 + \sum_{m \geq 1} f(n-1, m)x^m + \sum_{m \geq 1} f(n-1, m-1)x^m \\ &= F_{n-1}(x) + xF_{n-1}(x) = (1+x)F_{n-1}(x). \end{aligned}$$

By induction it follows that  $F_n(x) = (1+x)^n$ . Thus,

$$f(n, m) = \text{CF}[x^m, (1+x)^n] = \begin{cases} C(n, m) & \text{if } 0 \leq m \leq n \\ 0 & \text{if } m > n. \end{cases}$$

**Alternate.** For  $m > 0$ , define  $G_m(y) = \sum_{n \geq 0} f(n, m)y^n = \sum_{n \geq 1} f(n, m)y^n$ . Then,  $G_1(y) = \frac{y}{(1-y)^2}$ , and for  $m \geq 2$ , Equation (6.10) gives

$$\begin{aligned} G_m(y) &= \sum_{n \geq 1} f(n, m)y^n = \sum_{n \geq 1} (f(n-1, m) + f(n-1, m-1))y^n \\ &= \sum_{n \geq 1} f(n-1, m)y^n + \sum_{n \geq 1} f(n-1, m-1)y^n \\ &= yG_m(y) + yG_{m-1}(y). \end{aligned}$$

Therefore,  $G_m(y) = \frac{y}{1-y}G_{m-1}(y)$ . As  $G_1(y) = \frac{y}{(1-y)^2}$ , one has  $G_m(y) = \frac{y^m}{(1-y)^{m+1}}$ . Thus,

$$f(n, m) = \text{CF}\left[y^n, \frac{y^m}{(1-y)^{m+1}}\right] = \text{CF}\left[y^{n-m}, \frac{1}{(1-y)^{m+1}}\right] = \begin{cases} C(n, m) & \text{if } 0 \leq m \leq n \\ 0 & \text{if } m > n. \end{cases}$$

4. Determine the sequence  $\{S(n, m) : n, m \in \mathbb{W}\}$  which satisfies  $S(0, 0) = 1$ ,  $S(n, 0) = 0$  for  $n > 0$ ,  $S(0, m) = 0$  for  $m > 0$ , and

$$S(n, m) = mS(n-1, m) + S(n-1, m-1), \quad \text{for } n > 0, m > 0. \quad (6.11)$$

Answer: For  $n > 0$ , define  $G_m(y) = \sum_{n \geq 0} S(n, m)y^n = \sum_{n \geq 1} S(n, m)y^n$ . Then  $G_1(y) = \frac{y}{1-y}$ , and for  $m \geq 1$ , Equation (6.11) gives

$$\begin{aligned} G_m(y) &= \sum_{n \geq 0} S(n, m)y^n = \sum_{n \geq 1} (mS(n-1, m) + S(n-1, m-1))y^n \\ &= m \sum_{n \geq 1} S(n-1, m)y^n + \sum_{n \geq 1} S(n-1, m-1)y^n \\ &= myG_m(y) + yG_{m-1}(y). \end{aligned}$$

Therefore,  $G_m(y) = \frac{y}{1-my}G_{m-1}(y)$ . By induction it follows that

$$G_m(y) = \frac{y^m}{(1-y)(1-2y)\cdots(1-my)} = y^m \sum_{k=1}^m \frac{\alpha_k}{1-ky},$$

where  $\alpha_k = \frac{(-1)^{m-k} k^m}{k! (m-k)!}$  for  $1 \leq k \leq m$ . Then

$$\begin{aligned} S(n, m) &= \text{CF} \left[ y^n, y^m \sum_{k=1}^m \frac{\alpha_k}{1-ky} \right] = \sum_{k=1}^m \text{CF} \left[ y^{n-m}, \frac{\alpha_k}{1-ky} \right] \\ &= \sum_{k=1}^m \alpha_k k^{n-m} = \sum_{k=1}^m \frac{(-1)^{m-k} k^n}{k! (m-k)!} \\ &= \frac{1}{m!} \sum_{k=1}^m (-1)^{m-k} k^n C(m, k) = \frac{1}{m!} \sum_{k=1}^m (-1)^k (m-k)^n C(m, k). \end{aligned}$$

(a) The identity  $S(n, m) = \frac{1}{m!} \sum_{k=1}^m (-1)^k (m-k)^n C(m, k)$  is known as the **Stirling's Identity**.

(b) As there is no restriction on  $n, m \in \mathbb{N}_0$ , Equation (6.13) is also valid for  $n < m$ . But, we know that  $S(n, m) = 0$ , whenever  $n < m$ . Hence, we get the following identity,

$$\sum_{k=1}^m \frac{(-1)^{m-k} k^{n-1}}{(k-1)! (m-k)!} = 0 \text{ whenever } n < m.$$

5. **[Bell Numbers]** Recall that the  $n$ -th Bell number  $b(n)$  for  $n \in \mathbb{N}$ , is the number of partitions of  $\{1, 2, \dots, n\}$ . By convention we take  $b(0) = 1$ . For  $n \geq 1$ ,

$$\begin{aligned} b(n) &= \sum_{m=1}^n S(n, m) = \sum_{m \geq 1} S(n, m) = \sum_{m \geq 1} \sum_{k=1}^m \frac{(-1)^{m-k} k^{n-1}}{(k-1)! (m-k)!} \\ &= \sum_{k \geq 1} \frac{k^n}{k!} \sum_{m \geq k} \frac{(-1)^{m-k}}{(m-k)!} = \frac{1}{e} \sum_{k \geq 1} \frac{k^n}{k!} = \frac{1}{e} \sum_{k \geq 0} \frac{k^n}{k!} \end{aligned}$$

as  $0^n = 0$  for  $n \geq 1$ . We see that Equation (6.14) is valid even for  $n = 0$ . Notice that  $b(n)$  has terms of the form  $\frac{k^n}{k!}$ . So, we compute its egf as follows:

$$\begin{aligned} B(x) &= 1 + \sum_{n \geq 1} b(n) \frac{x^n}{n!} = 1 + \sum_{n \geq 1} \left( \frac{1}{e} \sum_{k \geq 1} \frac{k^n}{k!} \right) \frac{x^n}{n!} \\ &= 1 + \frac{1}{e} \sum_{k \geq 1} \frac{1}{k!} \sum_{n \geq 1} k^n \frac{x^n}{n!} = 1 + \frac{1}{e} \sum_{k \geq 1} \frac{1}{k!} \sum_{n \geq 1} \frac{(kx)^n}{n!} \\ &= 1 + \frac{1}{e} \sum_{k \geq 1} \frac{1}{k!} (e^{kx} - 1) = 1 + \frac{1}{e} \sum_{k \geq 1} \left( \frac{(e^x)^k}{k!} - \frac{1}{k!} \right) \\ &= 1 + \frac{1}{e} (e^{e^x} - 1 - (e - 1)) = e^{e^x - 1}. \end{aligned}$$

Recall that  $e^{e^x - 1}$  is a valid formal power series (see Remark 6.3.5). Taking logarithm of Equation (6.15), we get  $\log B(x) = e^x - 1$ . Hence,  $B'(x) = e^x B(x)$ , or equivalently

$$B'(x) = \sum_{n \geq 1} \frac{b(n)x^{n-1}}{(n-1)!} = e^x \sum_{n \geq 0} b(n) \frac{x^n}{n!} = \sum_{m \geq 0} \frac{x^m}{m!} \cdot \sum_{n \geq 0} b(n) \frac{x^n}{n!}.$$

Thus,

$$\frac{b(n)}{(n-1)!} = \text{CF}[x^{n-1}, B'(x)] = \text{CF} \left[ x^{n-1}, \sum_{m \geq 0} \frac{x^m}{m!} \cdot \sum_{n \geq 0} b(n) \frac{x^n}{n!} \right] = \sum_{m=0}^{n-1} \frac{1}{(n-1-m)!} \cdot \frac{b(m)}{m!}.$$

Therefore,  $b(n) = \sum_{m=0}^{n-1} C(n-1, m)b(m)$  for  $n \geq 1$ .

**EXERCISE 5.5.1.** Find the recurrence relation(s) for the number of binary words without having sub-words 00 and 111.

2. Find the number of subsets (including the empty set) of  $\{1, \dots, n\}$  not containing consecutive integers.
3. Let  $F_n$  be the  $n$ th Fibonacci number. Prove that if  $n, m \in \mathbb{N}$ , then  $F_n$  divides  $F_{nm}$ .
4. In a particular semester 6 students took admission in our PhD program. There were 9 professors who were willing to supervise these students. As a rule 'a student can have either one or two supervisors'. In how many ways can we allocate supervisors to these students if all the 'willing professors' are to be allocated? What if we have an additional condition that exactly one supervisor gets to supervise two students?
5. (a) Prove combinatorially that  $D_n = (n-1)(D_{n-1} + D_{n-2})$  for  $n \geq 2$ .  
 (b) Use (a) to show that the egf of  $D_n$  is  $\frac{e^{-x}}{1-x}$ .
6. (a) In how many ways can one distribute 10 identical chocolates among 10 students?  
 (b) In how many ways can one distribute 10 distinct chocolates among 10 students?  
 (c) In how many ways can one distribute 10 distinct chocolates among 10 students so that each receives one?  
 (d) In how many ways can one distribute 15 distinct chocolates among 10 students so that each receives at least one?  
 (e) In how many ways can one distribute 10 out of 15 distinct chocolates among 10 students so that each receives one?  
 (f) In how many ways can one distribute 15 distinct chocolates among 10 students so that each receives at most three?  
 (g) In how many ways can one distribute 15 distinct chocolates among 10 students so that each receives at least one and at most three?  
 (h) In how many ways can one distribute 15 identical chocolates among 10 students so that each receives at most three?
7. (a) In how many ways can one carry 15 distinct objects with 10 identical bags? Answer using  $S(n, r)$ .  
 (b) In how many ways can one carry 15 distinct objects in 10 identical bags with no empty bag? Answer using  $S(n, r)$ .  
 (c) In how many ways can one carry 15 distinct objects in 10 identical bags with each bag containing at most three objects?  
 (d) In how many ways can one carry 15 identical objects in 10 identical bags?  
 (e) In how many ways can one carry 15 identical objects in 10 identical bags with no empty bag?  
 (f) In how many ways can one carry 15 identical objects in 20 identical bags?
8. What is the number of integer solutions of  $x + y + z = 10$  with  $x \geq -1$ ,  $y \geq -2$  and  $z \geq -3$ ?
9. Is the number of solutions of  $x + y + z = 10$  in non-negative multiples of  $\frac{1}{2}$  ( $x, y, z$  are allowed to be  $0, 1/2, 1, 3/2, \dots$ ) at most four times the number of non-negative integer solutions of  $x + y + z = 10$ ?
10. How many words of length 8 can be formed using the English alphabet, where each letter can appear at most twice? Give answer using generating function.

11. Let  $p_1, \dots, p_n, n \geq 2$ , be distinct prime numbers. In how many ways can we partition the set  $\{p_1, \dots, p_n, p_1^2, \dots, p_n^2\}$  into subsets of size two such that no prime is in the same subset containing its square?
12. What is the value of  $\sum_{k=0}^{15} (-1)^k C(15, k)(15 - k)^5$ ?
13. Give your answers to the following questions using generating functions:
  - (a) What is the number of partitions of  $n$  with entries at most  $r$ ?
  - (b) What is the number of partitions of  $n$  with at most  $r$  parts?
  - (c) What is the number of partitions of  $n$  with exactly  $r$  parts ( $\pi_n(r)$ )?
  - (d) What is the number of partitions of  $n + C(r, 2)$  with  $r$  distinct parts?
  - (e) What is the number of partitions of  $n$  with distinct entries?
  - (f) What is the number of partitions of  $n$  with odd entries?
  - (g) What is the number of partitions of  $n$  with distinct odd entries?
  - (h) What is the number of self conjugate partitions of  $n$ ?
14. We summarize our findings about partitions in the following table.

Objects- $n$ distinct?	Places- $r$ distinct?	Places nonempty?	Relate	Number
Y	Y	Y	Onto functions	$r!S(n, r) = \sum_{i=0}^{r-1} (-1)^i C(r, i)(r - i)^n$
Y	Y	N	All functions	$r^n$
Y	N	Y	$r$ -partition of a set	$S(n, r)$
Y	N	N	All partitions of a set	$b(n) = \sum_{i=1}^r S(n, i)$
N	Y	Y	Positive integer solutions	$C(n - 1, r - 1)$
N	Y	N	Nonnegative integer solutions	$C(n + r - 1, r - 1)$
N	N	Y	$r$ -partition of $n$	$\pi_n(r) = \text{CF} \left[ x^{n-r}, \frac{1}{(1-x)(1-x^2)\dots(1-x^r)} \right]$
N	N	N	Partitions of $n$ of length $\leq r$	$\sum_{i=1}^r \pi_n(i)$

15. How many words of length 15 are there using the letters A,B,C,D,E such that each letter must appear in the word and A appears an even number of times? Give your answers using generating function.
16. The characteristic roots of an LHRC are 2, 2, 2, 3, 3. What is the form of the general solution?
17. Consider the LNRC  $a_n = c_1 a_{n-1} + \dots + c_r a_{n-r} + 5^n$ . Give a particular solution.
18. Obtain the ogf for  $a_n$ , where  $a_n = 2a_{n-1} - a_{n-2} + 2^n, a_0 = 0, a_1 = 1$ .
19. Solve the recurrence relation  $a_n = 2a_{n-1} - a_{n-2} + 2^n + 5, a_0 = 0, a_1 = 1$ .



20. Find the number of words of size 12 made using letters from  $\{A, B, C\}$  which do not have the sub-word  $BCA$ . For instance,  $BCCABCCABCCA$  is such a word, but  $ABCABCCCCCBA$  is not.
21. Find the number of 8 letter words made using letters from  $\{A, B, C, D\}$  in which 3 consecutive letters are not allowed to be the same.
22. We have 3 blue bags, 4 red bags and 5 green bags. We have many balls of each of the colors blue, red and green. What is the the smallest positive integer  $n$  so that if we distribute  $n$  balls (without seeing the colors) into these bags, then at least one of the following three conditions is met?  
Condition 1: A blue bag contains 3 blue balls or 4 red balls or 5 green balls.  
Condition 2: A red bag contains 3 blue balls or 5 red balls or 7 green balls.  
Condition 3: A green bag contains 3 blue balls or 6 red balls or 9 green balls.
23. Let  $f(x)$  be a polynomial with integer coefficients. What is the smallest natural number  $n$  such that if  $f(x) = 2009$  has  $n$  distinct integer roots, then  $f(x) = 9002$  does not have an integer root?
24. My friend says that he has  $n \geq 2$  subsets of  $\{1, 2, \dots, 14\}$  each of which has size 6. Give a value of  $n$  so that we can guarantee 'some two of his subsets have 3 elements in common', without seeing his collection? What is the smallest possible value of  $n$ ?
25. My class has  $n$  CSE,  $m$  MSC and  $r$  MC students. Suppose that  $t$  copies of the same book are to be distributed so that each branch gets at least  $s$  copies. In how many ways can this be done, if each student gets at most one? In how many ways can this be done, without the previous restriction? Answer using generating functions.
26. My class has  $n$  CSE,  $m$  MSC and  $r$  MC students. Suppose that  $t$  distinct books are to be distributed so that each branch gets at least  $s$ . In how many ways can this be done, if each student gets at most one? In how many ways can this be done, without the previous restriction? Answer only using generating function.
27. My class has  $N$  students. To conduct an exam, we have  $M$  identical answer scripts. In how many ways can we distribute the answer scripts so that each student gets at least 2. Answer using generating functions.
28. My class has  $N$  students. In an examination paper, there are  $M$  questions. Each student answers all the questions in an order decided by him/her. In how many ways can it happen that some three or more students have followed the same order? Answer using generating function.
29. Eleven teachers attended the Freshers' Party. There were 4 types of soft drinks available. In how many ways a total of 18 glasses of soft drinks can be served to them, in general? Answer using generating function.

## UNIT 5

## GRAPH THEORY: BASIC DEFINITIONS AND THEOREMS

## 1. DEFINITIONS

**Definition 1.** A graph  $G = (V, E)$  consists of a set  $V$  of **vertices** (also called **nodes**) and a set  $E$  of **edges**.

**Definition 2.** If an edge connects to a vertex we say the edge is **incident** to the vertex and say the vertex is an **endpoint** of the edge.

**Definition 3.** If an edge has only one endpoint then it is called a **loop edge**.

**Definition 4.** If two or more edges have the same endpoints then they are called **multiple** or **parallel** edges.

**Definition 5.** Two vertices that are joined by an edge are called **adjacent** vertices.

**Definition 6.** A **pendant** vertex is a vertex that is connected to exactly one other vertex by a single edge.

**Definition 7.** A **walk** in a graph is a sequence of alternating vertices and edges  $v_1e_1v_2e_2 \dots v_n e_n v_{n+1}$  with  $n \geq 0$ . If  $v_1 = v_{n+1}$  then the walk is **closed**. The **length** of the walk is the number of edges in the walk. A walk of length zero is a **trivial walk**.

**Definition 8.** A **trail** is a walk with no repeated edges. A **path** is a walk with no repeated vertices. A **circuit** is a closed trail and a **trivial circuit** has a single vertex and no edges. A trail or circuit is **Eulerian** if it uses every edge in the graph.

**Definition 9.** A **cycle** is a nontrivial circuit in which the only repeated vertex is the first/last one.

**Definition 10.** A **simple graph** is a graph with no loop edges or multiple edges. Edges in a simple graph may be specified by a set  $\{v_i, v_j\}$  of the two vertices that the edge makes adjacent. A graph with more than one edge between a pair of vertices is called a **multigraph** while a graph with loop edges is called a **pseudograph**.

**Definition 11.** A **directed graph** is a graph in which the edges may only be traversed in one direction. Edges in a simple directed graph may be specified by an ordered pair  $(v_i, v_j)$  of the two vertices that the edge connects. We say that  $v_i$  is **adjacent to**  $v_j$  and  $v_j$  is **adjacent from**  $v_i$ .

**Definition 12.** The **degree** of a vertex is the number of edges incident to the vertex and is denoted  $\deg(v)$ .

**Definition 13.** In a directed graph, the **in-degree** of a vertex is the number of edges **incident to** the vertex and the **out-degree** of a vertex is the number of edges **incident from** the vertex.

**Definition 14.** A graph is **connected** if there is a walk between every pair of distinct vertices in the graph.

**Definition 15.** A graph  $H$  is a **subgraph** of a graph  $G$  if all vertices and edges in  $H$  are also in  $G$ .

**Definition 16.** A **connected component** of  $G$  is a connected subgraph  $H$  of  $G$  such that no other connected subgraph of  $G$  contains  $H$ .

**Definition 17.** A graph is called **Eulerian** if it contains an Eulerian circuit.

**Definition 18.** A **tree** is a connected, simple graph that has no cycles. Vertices of degree 1 in a tree are called the **leaves** of the tree.

**Definition 19.** Let  $G$  be a simple, connected graph. The subgraph  $T$  is a **spanning tree of**  $G$  if  $T$  is a tree and every node in  $G$  is a node in  $T$ .

**Definition 20.** A **weighted graph** is a graph  $G = (V, E)$  along with a function  $w : E \rightarrow \mathbb{R}$  that associates a numerical weight to each edge. If  $G$  is a weighted graph, then  $T$  is a **minimal spanning tree of**  $G$  if it is a spanning tree and no other spanning tree of  $G$  has smaller total weight.

**Definition 21.** The **complete graph** on  $n$  nodes, denoted  $K_n$ , is the simple graph with nodes  $\{1, \dots, n\}$  and an edge between every pair of distinct nodes.

**Definition 22.** A graph is called **bipartite** if its set of nodes can be partitioned into two disjoint sets  $S_1$  and  $S_2$  so that every edge in the graph has one endpoint in  $S_1$  and one endpoint in  $S_2$ .

**Definition 23.** The **complete bipartite graph** on  $n, m$  nodes, denoted  $K_{n,m}$ , is the simple bipartite graph with nodes  $S_1 = \{a_1, \dots, a_n\}$  and  $S_2 = \{b_1, \dots, b_m\}$  and with edges connecting each node in  $S_1$  to every node in  $S_2$ .

**Definition 24.** Simple graphs  $G$  and  $H$  are called **isomorphic** if there is a bijection  $f$  from the nodes of  $G$  to the nodes of  $H$  such that  $\{v, w\}$  is an edge in  $G$  if and only if  $\{f(v), f(w)\}$  is an edge of  $H$ . The function  $f$  is called an **isomorphism**.

**Definition 25.** A simple, connected graph is called **planar** if there is a way to draw it on a plane so that no edges cross. Such a drawing is called an **embedding** of the graph in the plane.

**Definition 26.** For a planar graph  $G$  embedded in the plane, a **face** of the graph is a region of the plane created by the drawing. The area of the plane outside the graph is also a face, called the unbounded face.

## GRAPH THEORY: BASIC DEFINITIONS AND THEOREMS

## THEOREMS

**Theorem 1.** *Let  $G$  be a connected graph. Then  $G$  is Eulerian if and only if every vertex in  $G$  has even degree.*

**Theorem 2** (Handshaking Lemma). *In any graph with  $n$  vertices  $v_i$  and  $m$  edges*

$$\sum_{i=1}^n \deg(v_i) = 2m$$

**Corollary 1.** *A connected non-Eulerian graph has an Eulerian trail if and only if it has exactly two vertices of odd degree. The trail begins and ends these two vertices.*

**Theorem 3.** *If  $T$  is a tree with  $n$  edges, then  $T$  has  $n + 1$  vertices.*

**Theorem 4.** *Two graphs that are isomorphic to one another must have*

- (1) *The same number of nodes.*
- (2) *The same number of edges.*
- (3) *The same number of nodes of any given degree.*
- (4) *The same number of cycles.*
- (5) *The same number of cycles of any given size.*

**Theorem 5** (Kuratowski's Theorem). *A graph  $G$  is nonplanar if and only if it contains a "copy" of  $K_{3,3}$  or  $K_5$  as a subgraph.*

**Theorem 6** (Euler's Formula for Planar Graphs). *For any connected planar graph  $G$  embedded in the plane with  $V$  vertices,  $E$  edges, and  $F$  faces, it must be the case that*

$$V + F = E + 2.$$

# Graphs and Subgraphs

## 1.1 Introduction

Graph theory is a branch of mathematics which deals the problems, with the help of diagrams. There are many applications of graph theory to a wide variety of subjects which include operations research, physics, chemistry, computer science and other branches of science. In this chapter we introduce some basic concepts of graph theory and provide variety of examples. We also obtain some elementary results.

## 1.2 What is a graph ?

**Definition 1.2.1.** A *graph*  $G$  consists of a pair  $(V(G), X(G))$  where  $V(G)$  is a non empty finite set whose elements are called **points or vertices** and  $X(G)$  is a set of unordered pairs of distinct elements of  $V(G)$ . The elements of  $X(G)$  are called **lines or edges** of the graph  $G$ . If  $x = \{u, v\} \in X(G)$ , the line  $x$  is said to join  $u$  and  $v$ . We write  $x = uv$  and we say that the points  $u$  and  $v$  are **adjacent**. We also say that the point  $u$  and the line  $x$  are incident with each other. If two lines  $x$  and  $y$  are incident with a common point then they are called **adjacent lines**. A graph with  $p$  points and  $q$  lines is called a  $(p, q)$  *graph*. When there is no possibility of confusion we write  $V(G) = V$  and  $X(G) = X$ .

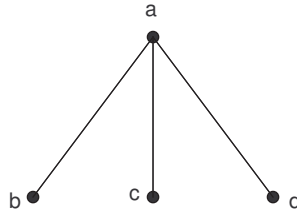


Figure 1.1: A an example of a  $(4, 3)$  graph

### 1.3 Representation of a graph

It is customary to represent a graph by a diagram and refer to the diagram itself as the graph. Each point is represented by a small dot and each line is represented by a line segment joining the two points with which the line is incident. Thus a diagram of graph depicts the incidence relation holding between its points and lines. In drawing a graph it is immaterial whether the lines are drawn straight or curved, long or short and what is important is the incidence relation between its points and lines.

#### Example 1.3.1.

1. Let  $V = \{a, b, c, d\}$  and  $X = \{\{a, b\}, \{a, c\}, \{a, d\}\}$ ,  $G = (V, X)$  is a  $(4, 3)$  graph. This graph can be represented by the diagram given in figure 1.1. In this graph the points  $a$  and  $b$  are adjacent whereas  $b$  and  $c$  are nonadjacent.
2. Let  $V = \{1, 2, 3, 4\}$  and  $X = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$ . Then  $G = (V, X)$  is a  $(4, 6)$  graph. This graph is represented by the diagram given in figure 1.2. Although the lines  $\{1, 2\}$  and  $\{2, 4\}$  intersect in the diagram, their intersection is not a point of the graph. Figure 1.3 is another diagram for the graph given in figure 1.2.
3. The  $(10, 15)$  graph given in figure 1.4 is called the **Petersen graph**.

**Remark 1.3.1.** The definition of a graph does not allow more than one line joining two points. It also does not allow any line joining a point to itself. Such a line joining a point to itself is called a **loop**.

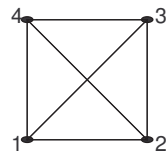


Figure 1.2: An example of a  $(4, 6)$  graph

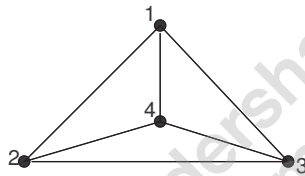


Figure 1.3: Another representation of graph shown in figure [1.1](#)

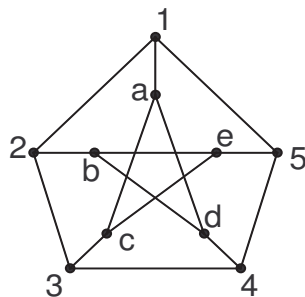


Figure 1.4: Petersen graph



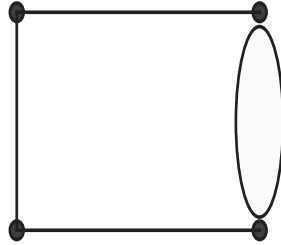


Figure 1.5: A multiple graph

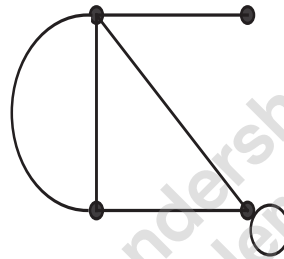


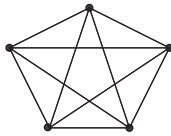
Figure 1.6: A pseudograph

**Definition 1.3.1.** If more than one line joining two vertices are allowed, the resulting object is called a **multigraph**. Line joining the same points are called **multi lines**. If further loops are also allowed, the resulting object is called **Pseudo graph**.

**Example 1.3.2.** Figure [1.5](#) is a multigraph and figure [1.6](#) is a pseudo graph.

**Remark 1.3.2.** Let  $G$  be a  $(p, q)$  graph. Then  $q \leq \binom{p}{2}$  and  $q = \binom{p}{2}$  iff any two distinct points are adjacent.

**Definition 1.3.2.** A Graph in which any two distinct points are adjacent is called a **complete graph**. The complete graph with  $p$  points is denoted by  $K_p$ .  $K_3$  is called a triangle. The graph given Fig. [1.3](#) is  $K_4$  and  $K_5$  is shown in Fig. [1.7](#)

Figure 1.7:  $K_5$ 

**Definition 1.3.3.** A graph whose edge set is empty is called a **null graph** or a **totally disconnected graph**.

**Definition 1.3.4.** A graph  $G$  is called labeled if its  $p$  points are distinguished from one another by names such as  $v_1, v_2 \cdots v_p$ .

The graphs given in Fig. 1.1 and Fig. 1.3 are labelled graphs and the graph in Fig. 1.7 is an unlabelled graph.

**Definition 1.3.5.** A graph  $G$  is called a **bigraph** or **bipartite graph** if  $V$  can be partitioned into two disjoint subsets  $V_1$  and  $V_2$  such that every line of  $G$  joins a point of  $V_1$  to a point of  $V_2$ .  $(V_1, V_2)$  is called a **bipartition** of  $G$ . If further  $G$  contains every line joining the points of  $V_1$  to the points of  $V_2$  then  $G$  is called a **complete bigraph**. If  $V_1$  contains  $m$  points and  $V_2$  contains  $n$  points then the complete bigraph  $G$  is denoted by  $K_{m,n}$ . The graph given in Fig. 1.1 is  $K_{1,3}$ . The graph given in Fig. 1.8 is  $K_{3,3}$ .  $K_{1,m}$  is called a **star** for  $m \geq 1$ .

## 1.4 Exercise

1. Draw all graphs with 1, 2, 3 and 4 points.
2. Find the number of points and lines in  $K_{m,n}$ .
3. Let  $V = \{1, 2, 3, \dots, n\}$ . Let  $X = \{ \{i, j\} \mid i, j \in V \text{ and are relatively prime} \}$ . The resulting graph  $(V, X)$  is denoted by  $G_n$ . Draw  $G_4$  and  $G_5$ .

## 1.5 Degrees

**Definition 1.5.1.** The **degree** of a point  $v_i$  in a graph  $G$  is the number of lines incident with  $v_i$ . The degree of  $v_i$  is denoted by  $d_G(v_i)$  or  $\deg v_i$  or  $d(v_i)$ .

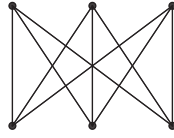


Figure 1.8: bigraph

A point  $v$  of degree 0 is called an **isolated point**. A point  $v$  of degree 1 is called an endpoint.

**Theorem 1.5.1.** The sum of the degrees of the points of a graph  $G$  is twice the number of lines. That is,  $\sum_i \deg v_i = 2q$ .

*Proof.* Every line of  $G$  is incident with two points. Hence every line contribute 2 to the sum of the degrees of the points. Hence  $\sum_i \deg v_i = 2q$ .  $\square$

**Corollary 1.5.1.** In any graph  $G$  the number of points of odd degree is even.

*Proof.* Let  $v_1, v_2, \dots, v_k$  denote the point of odd degree and  $w_1, w_2, \dots, w_m$  denote the points of even degree in  $G$ . By theorem [1.5.1](#),  $\sum_{i=1}^k \deg(v_i) + \sum_{i=1}^m \deg w_i = 2q$  which is even. Further  $\sum_{i=1}^m \deg w_i$  is even. Hence  $\sum_{i=1}^k \deg v_i$  is also even. But  $\deg v_i$  is odd for each  $i$ . Hence  $k$  must be even.  $\square$

**Definition 1.5.2.** For any graph  $G$ , we define

$$\delta(G) = \min\{\deg v/v \in V(G)\} \text{ and}$$

$$\Delta(G) = \max\{\deg v/v \in V(G)\}.$$

If all the points of  $G$  have the same degree  $r$ , then  $\delta(G) = \Delta(G) = r$  and this case  $G$  is called a **regular graph** of degree  $r$ . A regular graph of degree 3 is called a cubic graph. For example, the complete graph  $K_p$  is regular of degree  $p - 1$ .

**Theorem 1.5.2.** Every cubic graph has an even number of points.

*Proof.* Let  $G$  be a cubic graph with  $p$  points, then  $\sum \deg v = 3p$  which is even by theorem [1.5.1](#). Hence  $p$  is even.  $\square$

## Solved Problems

**Problem 1.** Let  $G$  be a  $(p, q)$  graph all of whose points have degree  $k$  or  $k + 1$ . If  $G$  has  $t > 0$  points of degree  $k$ , show that  $t = p(k + 1) - 2q$ .

**Solution**

Since  $G$  has  $t$  points of degree  $k$ , the remaining  $p - t$  points have degree  $k + 1$ . Hence  $\sum_{v \in V} d(v) = tk + (p - t)(k + 1)$ .

$$\therefore tk + (p - t)(k + 1) = 2q$$

$$\therefore t = p(k + 1) - 2q.$$

**Problem 2.** Show that in any group of two or more people, there are always two with exactly the same number of friends inside the group.

**Solution.** We construct a graph  $G$  by taking the group of people as the set of points and joining two of them if they are friends, then  $\deg v$  is equal to number of friends of  $v$  and hence we need only to prove that at least two points of  $G$  have the same degree. Let  $V(G) = \{v_1, v_2, \dots, v_p\}$ . Clearly  $0 \leq \deg v_i \leq p - 1$  for each  $i$ . Suppose no two points of  $G$  have the same degree. Then the degrees of  $v_1, v_2, \dots, v_p$  are the integers  $0, 1, 2, \dots, p - 1$  in some order. However a point of degree  $p - 1$  is joined to every other point of  $G$  and hence no point can have degree zero which is a contradiction. Hence there exist two points of  $G$  with equal degree.

**Problem 3.** Prove that  $\delta \leq 2q/p \leq \Delta$

**Solution**

Let  $V(G) = \{v_1, v_2, \dots, v_p\}$ . We have  $\delta \leq \deg v_i \leq \Delta$ . for all  $i$ . Hence

$$p\delta \leq \sum_{i=1}^p \deg v_i \leq p\Delta.$$

$$\therefore p\delta \leq 2q \leq p\Delta \text{ (by theorem 2.1)}$$

$$\therefore \delta \leq \frac{2q}{p} \leq \Delta$$

**Problem 4.** Let  $G$  be a  $k$ -regular bipartite graph with bipartition  $(V_1, V_2)$  and  $k > 0$ . Prove that  $|V_1| = |V_2|$ .

**Solution**

Since every line of  $G$  has one end in  $V_1$  and other end in  $V_2$  it follows that

$\sum_{v \in V_1} d(v) = \sum_{v \in V_2} d(v) = q$ . Also  $d(v) = k$  for all  $v \in V = V_1 \cup V_2$ . Hence  $\sum_{v \in V_1} d(v) = k|V_1|$  and  $\sum_{v \in V_2} d(v) = k|V_2|$  so that  $k|V_1| = k|V_2|$ . Since  $k > 0$ , we have  $|V_1| = |V_2|$ .

## 1.7 Exercise

1. Given an example of a regular graph of degree 0
2. Give three examples for a regular graph of degree 1
3. Give three examples for a regular graph of degree 2
4. What is the maximum degree of any point in a graph with  $p$  points?
5. Show that a graph with  $p$  points is regular of degree  $p - 1$  if and only if it is complete
6. Let  $G$  be a graph with at least two points show that  $G$  contains two vertices of the same degree
7. A  $(p, q)$  graph has  $t$  points of degree  $m$  and all other points are of degree  $n$ . Show that  $(m - n)t + pn = 2q$ .

## 1.8 Subgraphs

**Definition 1.8.1.** A graph  $H = (V_1, X_1)$  is called **subgraph** of  $G = (V, X)$ .  $V_1 \subseteq V$  and  $X_1 \subseteq X$ . If  $H$  is a subgraph of  $G$  we say that  $G$  is a **supergraph** of  $H$ .  $H$  is called a **spanning subgraph** of  $G$  if  $H$  is the maximal subgraph of  $G$  with point set  $V_1$ . Thus, if  $H$  is an induced subgraph of  $G$ , two points are adjacent in  $H$  they are adjacent in  $G$ . If  $V_2 \subseteq V$ , then the induced subgraph of  $G$  induced by  $V_2$  and is denoted by  $G[V_2]$ . If  $X_2 \subseteq X$ , then the sub graph of  $G$  with line set  $X_2$  and is denoted by  $G[X_2]$

**Examples.** Consider the Petersen graph  $G$  given in Fig. 1.4. The graph given in Fig. 1.9 is a subgraph of  $G$ . The graph given in Fig. 1.10 is an induced subgraph of  $G$ . The graph given in Fig. 1.11 is an induced subgraph of  $G$ . The graph given in Fig. 1.12 is a spanning subgraph of  $G$ .

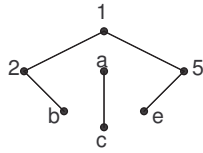


Figure 1.9: Subgraph

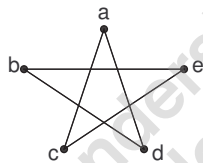


Figure 1.10: Induced subgraph

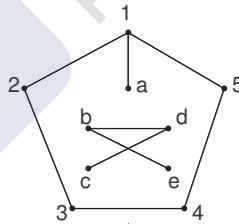


Figure 1.11: Spanning subgraph

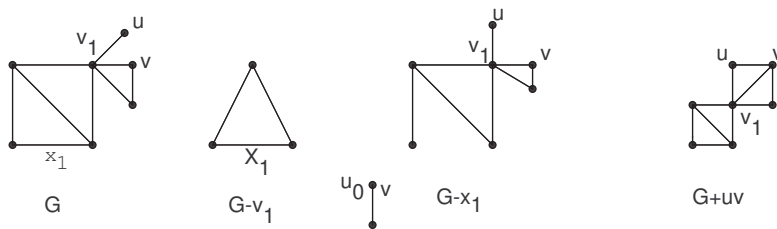


Figure 1.12:

**Definition 1.8.2.** Let  $G = (V, X)$  be a graph. Let  $v_i \in V$ . The subgraph of  $G$  obtained by removing the point  $v_i$  and all the lines incident with  $v_i$  is called the **subgraph obtained by the removal of the point  $v_i$**  and is denoted by  $G - v_i$ . Thus if  $G - v_i = (V_i, X_i)$  then  $V_i = V - v_i$  and  $X_i = \{x/x \in X \text{ and } x \text{ is not incident with } v_i\}$ . Clearly  $G - v_i$  is an induced subgraph of  $G$ . Let  $x_i \in X$ . Then  $G - x_i = (V, X - x_i)$  is called the subgraph of  $G$  obtained by the removal of the line  $x_j$ . Clearly  $G - x_j$  is a spanning subgraph of  $G$  which contains all the lines of  $G$  except  $x_j$ . The removal of a set of points or lines from  $G$  is defined to be the removal of single elements in succession.

**Definition 1.8.3.** Let  $G = (V, X)$  be a graph. Let  $v_i, v_j$  be two points which are not adjacent in  $G$ . Then  $G + v_i v_j = (V, X \cup \{v_i, v_j\})$  is called the graph obtained by **the addition of the line  $v_i v_j$**  to  $G$

Clearly  $G + v_i v_j$  is the smallest super graph of  $G$  containing the line  $v_i v_j$ . We listed these concepts in Fig 1.12. The proof given in the following theorem is typical of several proofs in theory.

**Theorem 1.8.1.** The maximum number of lines among all  $p$  point graph no triangles is  $\left\lfloor \frac{p^2}{4} \right\rfloor$ . ( $\lfloor x \rfloor$  denotes the greatest integer not exceeding the the real number  $x$ ).

*Proof.* The result can be easily verified for  $p \leq 4$ . For  $p > 4$ , we will prove by induction separately for odd  $p$  and for every  $p$ .

**Part 1.** For odd  $p$ .

Suppose the result is true for all odd  $p \leq 2n + 1$ . Now let  $G$  be a  $(p, q)$  graph with  $p = 2n + 3$  and no triangles. If  $q = 0$ , then  $q \leq \left\lfloor \frac{p^2}{4} \right\rfloor$ . Hence let  $q > 0$ . Let  $u$  and  $v$  be a pair of adjacent points. The subgraph  $G' = G - \{u, v\}$  has

$2n + 1$  points and no triangles. Hence induction hypothesis,

$$\begin{aligned} q(G') &\leq \left\lfloor \frac{(2n+1)^2}{4} \right\rfloor = \left\lfloor \frac{4n^2 + 4n + 1}{4} \right\rfloor \\ &= \left\lfloor n^2 + n + \frac{1}{4} \right\rfloor = n^2 + n \end{aligned}$$

Since  $G$  has no triangles, no point of  $G'$  can be adjacent to both  $u$  and  $v$ . Now, lines in  $G$  are of three types.

1. Lines of  $G'$  ( $\leq n^2 + n$  in number by (1))
2. Lines between  $G'$  and  $\{u, v\}$  ( $\leq 2n + 1$  in number by (2))
3. Line  $uv$

Hence

$$\begin{aligned} q &\leq (n^2 + n) + (2n + 1) + 1 = n^2 + 3n + 2 \\ &= \frac{1}{4}(4n^2 + 12n + 8) \\ &= \left( \frac{4n^2 + 12n + 9}{4} - \frac{1}{4} \right) \\ &= \left\lfloor \frac{(2n+3)^2}{4} \right\rfloor = \left\lfloor \frac{p^2}{4} \right\rfloor \end{aligned}$$

Also for  $p = 2n + 3$ , the graph  $K_{n+1, n+2}$  has no triangles and has  $(n + 1)(n + 2) = n^2 + 3n + 2 = \left\lfloor \frac{p^2}{4} \right\rfloor$  lines. Hence this maximum  $q$  is attained.

**Part 2.** For even  $p$ .

Suppose the result is true for all even  $p \leq 2n$ . Now let  $G$  be a  $(p, q)$  graph with  $p = 2n + 2$  and no triangles. As before, let  $u$  and  $v$  be a pair of adjacent points in  $G$  and let  $G' = G - \{u, v\}$ .

Now  $G'$  has  $2n$  points and no triangles. Hence by hypothesis,

$$q(G') \leq \left\lfloor \frac{(2n)^2}{4} \right\rfloor = n^2$$

Lines in  $G$  are of three types.



- (i) Lines of  $G'$
- (ii) Lines between  $G'$  and  $\{u, v\}$
- (iii) line  $uv$ .

Hence  $q \leq n^2 + 2n + 1 = (n + 1)^2 = \frac{(2n+2)^2}{4} = \lfloor p^2/4 \rfloor$ . Hence the result holds for even  $p$  also. We see that for  $p = 2n + 2$ ,  $K_{n+1, n+1}$  is a  $(p, \lfloor p^2/4 \rfloor)$  graph without triangles.  $\square$

## 1.9 Exercise

1. Show that  $K_p - v = K_{p-1}$  for any point  $v$  of  $K_p$ .
2. Show that an induced subgraph of a complete graph is complete.
3. Let  $G = (V, X)$  be a  $(p, q)$  graph. Let  $v \in V$  and  $x \in X$ . Find the number of points and lines in  $G - v$  and  $G - x$ .
4. If every induced proper subgraph of a graph  $G$  is complete and  $p > 2$  then show that  $G$  is complete.
5. If every induced proper subgraph of a graph  $G$  is totally disconnected, then show that  $G$  is totally disconnected.
6. Show that in a graph  $G$  every induced graph is complete iff every induced graph with two points is complete.

## 1.10 Isomorphism

**Definition 1.10.1.** Two graphs  $G_1 = (V_1, X_1)$  and  $G_2 = (V_2, X_2)$  are said to be **isomorphic** if there exists a bijection  $f : V_1 \rightarrow V_2$  such that  $u, v$  are adjacent in  $G_1$  if and only if  $f(u), f(v)$  are adjacent in  $G_2$ . If  $G_1$  is isomorphic to  $G_2$ , we write  $G_1 \cong G_2$ . The map  $f$  is called an isomorphism from  $G_1$  to  $G_2$ .

- Example 1.10.1.**
1. The graph given in Fig. 2.2 and Fig. 2.3 are isomorphic.
  2. The two graphs given in Fig. 1.13 are isomorphic.  $f(u_i) = v_i$  is an isomorphism between these two graphs.

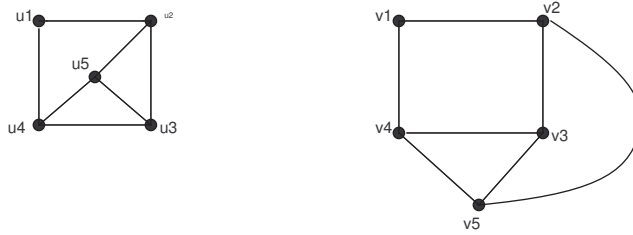


Figure 1.13:

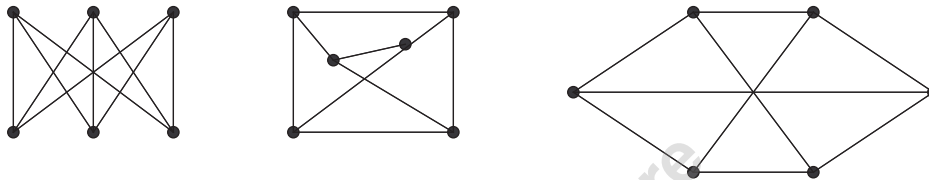


Figure 1.14:

3. The three graphs given in Fig 1.14 are isomorphic with each other.

**Theorem 1.10.1.** Let  $f$  be an isomorphism of the graph  $G_1 = (V_1, X_1)$  to the graph  $G_2 = (V_2, X_2)$ . Let  $v \in V_1$ . Then  $\deg v = \deg f(v)$ . i.e., isomorphism preserves the degree of vertices.

*Proof.* A point  $u \in V_1$  is adjacent to  $v$  in  $G_1$  iff  $f(u)$  is adjacent to  $f(v)$  in  $G_2$ . Also  $f$  is bijection. Hence the number of points in  $V_1$  which are adjacent to  $v$  is equal to the number of points in  $V_2$  which are adjacent to  $f(v)$ . Hence  $\deg v = \deg f(v)$ .  $\square$

**Remark 1.10.1.** Two isomorphic graphs have the same number of points and the same number of lines. Also it follows from Theorem 1.10.1 that two isomorphic graphs have equal number of points with a given degree. However these conditions are not sufficient to ensure that two graphs are isomorphic. For example consider the two graphs given in figure 1.15. By theorem 1.10.1 under any isomorphism  $w_4$  must correspond to  $v_3$ ;  $w_1, w_5, w_6$  must correspond to  $v_1, v_5, v_6$  in some order. The remaining two points  $w_2, w_3$  are adjacent whereas  $v_2, v_4$  are not adjacent. Hence there does not exist an isomorphism



Figure 1.15:



Figure 1.16:

between these two graphs. However both graphs have exactly one vertex of degree 3, three vertices of degree 1 and two vertices of degree 2.

**Definition 1.10.2.** An isomorphism of a graph  $G$  onto itself is called an **automorphism** of  $G$ .

**Remark 1.10.2.** Let  $\Gamma(G)$  denote the set of all automorphism of  $G$ . Clearly the identity map  $i : V \rightarrow V$  defined by  $i(v) = v$  is an automorphism of  $G$  so that  $i \in \Gamma(G)$ . Further if  $\alpha$  and  $\beta$  are automorphisms of  $G$  then  $\alpha.\beta$  and  $\alpha^{-1}$  are also automorphism of  $G$ . Hence  $\Gamma(G)$  is a group and is called the **automorphism group** of  $G$ .

**Definition 1.10.3.** Let  $G = (V, X)$  be a graph. The **complement**  $\overline{G}$  of  $G$  is defined to be the graph which has  $V$  as its set of points and two points are adjacent in  $\overline{G}$  iff they are not adjacent in  $G$ .  $G$  is said to be a **self complementary** graph if  $G$  is isomorphic to  $\overline{G}$ .

For example the graphs given in Fig [1.16](#) are self complementary graphs.

It has been conjectured by Ulam that the collection of vertex deleted sub-graphs  $G - v$  determines  $G$  upto isomorphism.

### Solved Problems

**Problem 5.** Prove that any self complementary graphs has  $4n$  or  $4n + 1$  points

**Solution.** Let  $G = (V(G), X(G))$  be a self complementary graph with  $p$  points.

Since  $G$  is self complementary,  $G$  is isomorphic to  $\overline{G}$ .

$\therefore |X(G)| = |X(\overline{G})|$ . Also

$$\begin{aligned}
 |X(G)| + |X(\overline{G})| &= \binom{p}{2} = \frac{p(p-1)}{2} \\
 \therefore 2|X(G)| &= \frac{p(p-1)}{2} \\
 \therefore |X(G)| &= \frac{p(p-1)}{4} \text{ is an integer.}
 \end{aligned}$$

Further one of  $p$  or  $p-1$  is odd. Hence  $p$  or  $p-1$  is a multiple of 4.  $\therefore p$  is of the form  $4n$  or  $4n+1$ .

**Problem 6.** Prove that  $\Gamma(G) = \Gamma(\overline{G})$ .

**Solution.** Let  $f \in \Gamma(G)$  and let  $u, v \in V(G)$ .

Then  $u, v$  are adjacent in  $\overline{G} \Leftrightarrow u, v$  are not adjacent in  $G$ .

$\Leftrightarrow f(u), f(v)$  are not adjacent in  $G$

(since  $f$  is an automorphism of  $G$ )

$\Leftrightarrow f(u), f(v)$  are adjacent in  $\overline{G}$ .

Hence  $f$  is an automorphism of  $\overline{G}$ .

$\therefore f \in \Gamma(\overline{G})$  and hence  $\Gamma(G) \subseteq \Gamma(\overline{G})$ .

Similarly  $\Gamma(\overline{G}) \subseteq \Gamma(G)$  so that  $\Gamma(G) = \Gamma(\overline{G})$ .

## 1.11 Exercise

1. Prove that any graph with  $p$  points is isomorphic to a subgraph of  $K_p$ .
2. Show that isomorphism is an equivalence relation among graphs.
3. Show that the two graphs given in Fig. 2.17 are not isomorphic.

# Eulerian graphs, Hamiltonian graphs

## 2.1 Eulerian graphs

**Definition 2.1.1.** A closed trail containing all the points and lines is called an eulerian trail. A graph having an eulerian trail is called an eulerian graph.

**Remark 2.1.1.** In an eulerian graph, for every pair of points  $u$  and  $v$  there exists at least two edge disjoint  $u - v$  trails and consequently there are at least two edge disjoint  $u - v$  paths. The graph shown in figure 2.1 is eulerian.

**Theorem 2.1.1.** If  $G$  is a graph in which the degree of every vertex is at least two then  $G$  contains a cycle.

*Proof.* First, we construct a sequence of verices  $v_1, v_2, v_3, \dots$  as follows. Choose any vertex  $v$ . Let  $v_1$  be any vertex adjacent to  $v$ . Let  $v_2$  be any vertex adjacent

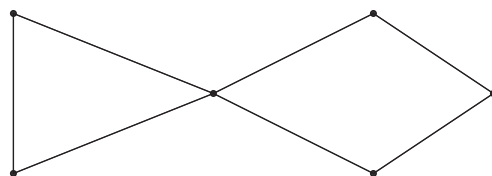


Figure 2.1: A Eulerian graph

to  $v_1$  other than  $v$ . At any stage, if the vertex  $v_i$ ,  $i \geq 2$  is already chosen, then choose  $v_{i+1}$  to be any vertex adjacent to  $v_i$  other than  $v_{i-1}$ . Since degree of each vertex is at least 2, the existence of  $v_{i+1}$  is always guaranteed.  $G$  has only finite number of vertices, at some stage we have to choose a vertex which has been chosen before. Let  $v_k$  be the first such vertex and let  $v_k = v_i$  where  $i < k$ . Then  $v_i v_{i+1} \dots v_k$  is a cycle.  $\square$

**Theorem 2.1.2.** Let  $G$  be a connected graph. Then the following statements are equivalent.

- (1)  $G$  is eulerian.
- (2) every point has even degree.
- (3) the set of edges of  $G$  can be partitioned into cycles.

*Proof.*

- (1)  $\Rightarrow$  (2) Assume that  $G$  is eulerian. Let  $T$  be an eulerian trail in  $G$ , with origin and terminus  $u$ . Each time a vertex  $v$  occurs in  $T$  in a place other than the origin and terminus, two of the edges incident with  $v$  are accounted for. Since an eulerian trail contains every edges of  $G$ ,  $d(v)$  is even for  $v \neq u$ . For  $u$ , one of the edges incident with  $u$  is accounted for by the origin of  $T$ , another by the terminus of  $T$  and others are accounted for in pairs. Hence  $d(u)$  is also even.
- (2)  $\Rightarrow$  (3) Since  $G$  is connected and nontrivial every vertex of  $G$  has degree at least 2. Hence  $G$  contains a cycle  $Z$ . The removal of the lines of  $Z$  results in a spanning subgraph  $G_1$  in which again vertex has even degree. If  $G_1$  has no edges, then all the lines of  $G$  form one cycle and hence (3) holds. Otherwise,  $G_1$  has a cycle  $Z_1$ . Removal of the lines of  $Z_1$  from  $G_1$  results in spanning subgraph  $G_2$  in which every vertex has even degree. Continuing the above process, when a graph  $G_n$  with no edge is obtained, we obtain a partition of the edges of  $G$  into  $n$  cycles.
- (3)  $\Rightarrow$  (1) If the partition has only one cycle, then  $G$  is obviously eulerian, since it is connected. Otherwise let  $z_1, z_2, \dots, z_n$  be the cycles forming a partition of the lines of  $G$ . Since  $G$  is connected there exists a cycle  $z_i \neq z_1$  having a common point  $v_1$  with  $z_1$ . Without loss of generality,

let it be  $z_2$ . The walk beginning at  $v_1$  and consisting of the cycles  $z_1$  and  $z_2$  in succession is a closed trail containing the edges of these two cycles. Continuing this process, we can construct a closed trail containing all the edges of  $G$ . Hence  $G$  is eulerian.

□

**Corollary 2.1.1.** Let  $G$  be a connected graph with exactly  $2n(n \geq 1)$ , odd vertices. Then the edge set of  $G$  can be partitioned into  $n$  open trails.

*Proof.* Let the odd vertices of  $G$  be labelled  $v_1, v_2, \dots, v_n; w_1, w_2, \dots, w_n$  in any arbitrary order. Add  $n$  edges to  $G$  between the vertex pairs  $(v_1, w_1), (v_2, w_2), \dots, (v_n, w_n)$  to form a new graph  $G'$ . No two of these  $n$  edges are incident with the same vertex. Further every vertex of  $G'$  is of even degree and hence  $G'$  has an eulerian trail  $T$ . If the  $n$  edges that we added to  $G$  are now removed from  $T$ , it will split into  $n$  open trails. These are open trails in  $G$  and form a partition of the edges of  $G$ .

□

**Corollary 2.1.2.** Let  $G$  be a connected graph with exactly two odd vertices. Then  $G$  has an open trail containing all the vertices and edges of  $G$ .

Corollary 2.1.2 answers the question: Which diagrams can be drawn without lifting one's pen from the paper not covering any line segment more than once?

**Definition 2.1.2.** A graph is said to be arbitrarily traversable (traceable) from a vertex  $v$  if the following procedure always results in an eulerian trail. Start at  $v$  by traversing any incident edge. On arriving at a vertex  $u$ , depart through any incident edge not yet traversed and continue until all the lines are traversed.

If a graph is arbitrarily traversable from a vertex then it obviously eulerian.

The graph shown in figure 2.1 is arbitrarily traversable from  $v$ . From no other point it is arbitrarily traversable.

**Theorem 2.1.3.** An eulerian graph  $G$  is arbitrarily traversable from a vertex  $v$  in  $G$  iff every cycle in  $G$  contains  $v$ .

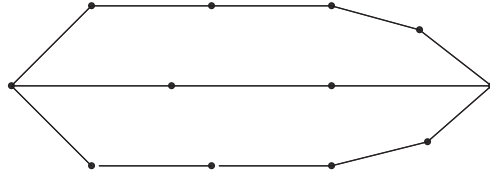


Figure 2.2: A theta graph

### 2.1.1 Exercise

1. For what values of  $n$ , is  $K_n$  eulerian?
2. For what values of  $m$  and  $n$  is  $K_{n,m}$  is eulerian?
3. Show that if  $G$  has no vertices of odd degree, then there are edge disjoint cycles  $C_1, C_2, \dots, C_n$  such that

$$E(G) = E(C_1) \cup E(C_2) \cup \dots \cup E(C_m)$$

4. Show that every block of a connected graph  $G$  is eulerian then  $G$  is eulerian.

## 2.2 Hamiltonian Graphs

**Definition 2.2.1.** A spanning cycle in a graph is called a hamiltonian cycle. A graph having a hamiltonian cycle is called a hamiltonian graph.

**Definition 2.2.2.** A block with two adjacent vertices of degree 3 and all other vertices of degree 2 is called a theta graph.

**Example 2.2.1.** The graph shown in figure 2.2 is a theta graph. A theta graph is obviously nonhamiltonian and every nonhamiltonian 2-connected graph has a theta subgraph.

**Theorem 2.2.1.** Every hamiltonian graph is 2-connected.

*Proof.* Let  $G$  be a hamiltonian graph and let  $Z$  be a hamiltonian cycle in  $G$ . For any vertex  $v$  of  $G$ ,  $Z - v$  is connected and hence  $G - v$  is also connected. Hence  $G$  has no cutpoints and thus  $G$  is 2-connected.  $\square$