Discrete Mathematics Course Notes

Felipe Balbi

March 1, 2020

Contents

Week 1 **5**
1.101 Introduction to discrete mathematics 5
1.104 The definition of a set 5
1.106 The listing method and rule of inclusion 7
1.108 The powerset of a set 7
1.110 Set operations 8

Week 2 **13**
1.201 The representation of a set using Venn diagrams 13
1.203 De Morgan's laws 15
1.205 Laws of sets: Commutative, associative and distributive 16
1.207 Partition 18

Week 3 **20**
2.101 Introduction 20
2.102 The Definition of A Function 20
2.104 Plotting functions 22
2.106 Injective and surjective functions 25

Week 4 **28**
2.201 Function composition 28
2.203 Bijective functions 29
2.205 Logarithmic functions 31
2.207 Floor and ceiling functions 32

Week 5 **35**
3.101 Introduction to propositional logic 35
3.103 Propositions 36
3.105 Truth tables and truth sets 37
3.107 Compound propositions 38

Week 6 **41**
3.202 Logical implication ($\rightarrow$) 41
3.204 Logical equivalence ($\leftrightarrow$) 43
3.206 Laws of propositional logic 45

Week 7 **46**
4.101 Introduction to predicate logic . . . 46
4.103 What are predicates? . . . 47
4.105 Quantification . . . 48
4.107 Nested Quantifiers . . . 50

Week 8 **52**
4.201 De Morgan's laws for quantifiers . . . 52
4.203 Rules of inference . . . 53
4.205 Rules of inference with quantifiers . . . 59

Week 9 **63**
5.101 Introduction to Boolean algebra . . . 63
5.103 Postulates of Boolean algebra . . . 65
5.105 Boolean functions . . . 67

Week 10 **70**
5.201 Logic gates . . . 70
5.203 Combinational circuits . . . 73
5.205 Simplification of circuits . . . 78

Week 11 **81**
6.101 Introduction to proofs . . . 81
6.103 The principle of mathematical induction . . . 83
6.106 Proof by induction . . . 84
6.108 Strong induction . . . 86

Week 12 **89**
6.201 Recursive definitions . . . 89
6.204 Recurrence relations . . . 90
6.206 Solving recurrence relations . . . 91

Week 13 **93**
7.101 Introduction . . . 93
7.103 Definition of a graph . . . 94
7.105 Walks and paths in a graph . . . 96
7.107 The degree sequence of a graph . . . 100
7.109 Special graphs: simple, r-regular and complete graphs . . . 102

Week 14 **105**
7.201 Isomorphic graphs . . . 105
7.203 Bipartite graphs . . . 105
7.205 The adjacency matrix of a graph . . . 107
7.207 Dijkstra's algorithm . . . 111

Week 15 **112**
8.103 Definition of a tree . . . 112
8.105 Spanning trees of a graph . . . 113
8.107 Minimum spanning tree . . . 116

Week 16 **117**
8.201 Rooted trees . . . 117
8.203 binary search trees . . . 120

Week 17 **122**
9.101 Introduction . . . 122
9.103 Definition of a relation: relation versus function . . . 123
9.105 Matrix and graph representations of a relation . . . 124
9.107 The properties of a relation: reflexive, symmetric and anti-symmetric . . . 126
9.109 Relation properties: transitivity . . . 129

Week 18 **132**
9.201 Equivalence relations and equivalence classes . . . 132
9.203 Partial and total order . . . 134

Week 19 **135**
10.101 Introduction . . . 135
10.103 The basics of counting . . . 135
10.105 The pigeonhole principle . . . 137
10.107 Permutations and combinations . . . 137

Week 20 **138**
10.201 Binomial coefficients and identities . . . 138
10.204 Generalised permutations and combinations . . . 140
10.206 Distinguishable objects and boxes . . . 141

Week 1

Learning objectives:

- Define a set, the elements of a set and the cardinality of a set.
- Define the concepts of the universal set and the complement of a set, and the difference between a set and a powerset of a set.
- Define the concepts of the union, intersection, set difference and symmetric difference, and the concept of a membership table.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.117–126
- Exercises

  pp.127–128 exercises 1–8 and 12–19.

For reading on set operations, please see the Essential reading for Week 2.

1.101 Introduction to discrete mathematics

The study of discrete objects. Such objects are separated or distant from each other.

We will study integers, propositions, sets, relations or functions.

We will learn their properties and relationships among them.

Sets, functions, logic, graphs, trees, relations, combinatorics, mathematical induction and recursive relations. We will gain mathematical understanding of these topics and that will improve our skill of thinking in abstract terms.

1.104 The definition of a set

Set Theory deals with properties of well-defined collection of objects. Introduced by George Cantor.

Forms the basis of other fields of study: counting theory, relations, graph theory and finite state machines.

Definition of a set

A collection of any kind of objects: people, ideas, numbers...

A set must be well-defined, meaning that there can be no ambiguity to which objects belongs to the set.

$$\begin{aligned} E &= \{2, 4, 6, 8\} \\ V &= \{a, e, i, o, u\} \\ EmptySet &= \{\} = \emptyset \end{aligned} \tag{0.1}$$

Definition 1 (Set)**.** *A set is an* ***unordered*** *collection of* ***unique*** *objects.*

Element of a set ($\in$)

Given the set $E = \{2, 4, 6, 8\}$ we can say $2 \in E$ (2 is an element of E) and $3 \notin E$ (3 is not an element of E)

Cardinality of a set (Card)

Definition 2 (Cardinality)**.** *Given a set S, the* ***cardinality*** *of S is the number of elements contained in S. We write the cardinality of S as $|S|$. Note that the cardinality of the empty set is zero ($|\emptyset| = 0$)*

Subset of a set ($\subseteq$)

Definition 3 (Subset)**.** *A is said to be a subset of B if and only if every element of A is also an element of B. In this case we write $A \subseteq B$.*

This means we have the following equivalence:

$$A \subseteq B \leftrightarrow \text{if x} \in A \,\text{then}\, x \in B(\text{for all x}) \tag{0.2}$$

The emptyset $\emptyset$ is a subset of any set.

Any set if a subset of itself ($S \subseteq S$)

Special Sets: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

$\mathbb{N}$: set of natural numbers

$\mathbb{Z}$: set of integers

$\mathbb{Q}$: set of rational numbers

$\mathbb{R}$: set of real numbers

1.106 The listing method and rule of inclusion

Two different ways of representing a set.

The listing method consists of simply listing all elements of a set.

$S_1 = \{1, 2, 3\}$

The rule of inclusion method consists of producing a rule such that when that rule is true, the element is a member of the set. For example, here's a rule of inclusion for the set of all **odd** integers:

$S_2 = \{2n + 1 \mid n \in \mathbb{Z}\}$

In some cases, the rule of inclusion (or set building notation) is the only way to actually describe a set. For example, if we were to try to list the elements of the set of rational numbers $\mathbb{Q}$, we would never be able to reach the end. However, with the set builder notation it becomes simple and concise:

$\mathbb{Q} = \{\frac{n}{m} \mid n, m \in \mathbb{Z} \text{and} m \neq 0\}$

We can use the same notation for the set of elements in my bag:

$S_{bag} = \{x \mid x \text{is in my bag}\}$

1.108 The powerset of a set

A set can contain other sets as elements. For example:

$$\begin{aligned} A &= \{1, 2, 3, 4, 5, 6, 7, 8, 9\} \\ B &= \{\{1, 2, 3, 4\}, \{5, 6\}, \{7, 8, 9\}\} \end{aligned} \tag{0.3}$$

Note that $\{1, 2, 3, 4\}$ is a **subset** of A but it is an **element** of B. In mathematical terms:

$$\{1, 2, 3, 4\} \subseteq A \,\text{but}\, \{1, 2, 3, 4\} \in B \tag{0.4}$$

Powerset of a set

Definition 4 (Powerset)**.** *Given a set S, the powerset of S, $P(S)$, is the set containing **all** the **subsets** of S*

1. Example 1

   Given a set $S = \{1, 2, 3\}$, the subsets of S are:

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

Therefore, the powerset of S, $P(S)$ is as follows:

$P(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

2. Example 2

   What is the powerset of the empty set? What is the powerset of the powerset of the empty set?

$$\begin{aligned} P(\emptyset) &= \{\emptyset\} \\ P(P(\emptyset)) &= \{\emptyset, \{\emptyset\}\} \end{aligned} \tag{0.5}$$

Cardinality of a powerset

Given a set S, then $|P(S)| = 2^{|S|}$

In other words: the cardinality of the powerset of S is the 2 to the power of the cardinality of S. For example:

$$\begin{aligned} S &= \{1,2\} \\ |S| &= 2 \\ P(S) &= \{\emptyset, \{1\}, \{2\}, \{1,2\}\} \\ |P(S)| &= 4 = 2^2 = 2^{|S|} \end{aligned} \tag{0.6}$$

1. Example

   Given a set A, if $|A| = n$ find $|P(P(P(A)))|$

$$\begin{aligned} |P(A)| &= 2^n \\ |P(P(A))| &= 2^{2^n} \\ |P(P(P(A)))| &= 2^{2^{2^n}} \end{aligned} \tag{0.7}$$

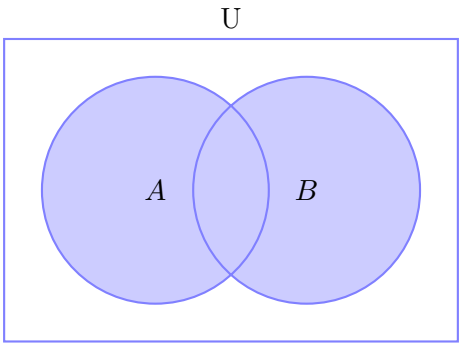
1.110 Set operations

We will look at set operations (intersection, union, difference, symmetric difference).

Union ($\cup$)

Definition 5 (Union)**.** *Given two sets A and B, the union of A and B, $A \cup B$, contains all the elements in **either** A or B.*

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\} \tag{0.8}$$



1. Example

$$\begin{aligned} A &= \{1, 2, 3\} \\ B &= \{4, 5, 6\} \\ A \cup B &= \{1, 2, 3, 4, 5, 6\} \end{aligned} \tag{0.9}$$

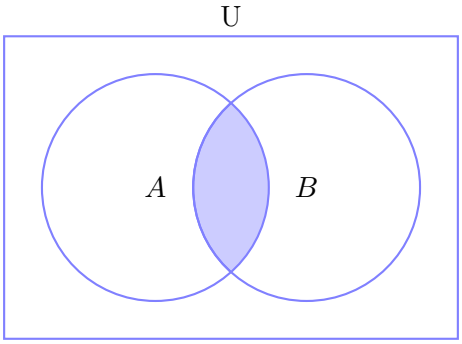
2. Membership Table ($A \cup B$)

A	B	$A \cup B$
0	0	0
0	1	1
1	0	1
1	1	1

Intersection ($\cap$)

Definition 6 (Intersection)**.** *Given two sets A and B, the intersection of A and B, $A \cap B$, contains all the elements in* ***both*** *A and B.*

$$A \cap B = \{x \mid x \in A \,\text{and}\, x \in B\} \tag{0.10}$$



;

1. Example

$$\begin{aligned} A &= \{1, 2, 3\} \\ B &= \{2, 3, 4\} \\ A \cap B &= \{2, 3, \} \end{aligned} \tag{0.11}$$

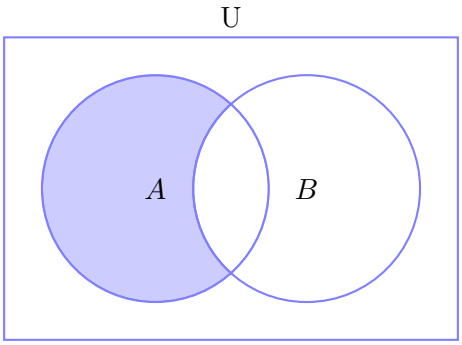
2. Membership Table ($A \cap B$)

A	B	$A \cap B$
0	0	0
0	1	0
1	0	0
1	1	1

Difference ($-$)

Definition 7 (Difference)**.** *Given two sets A and B, the difference of A and B, $A - B$, contains all the elements that are in A* ***but not*** *in B.*

$$A - B = \{x \mid x \in A \text{ and } x \notin B\} \tag{0.12}$$



1. Example

$$\begin{aligned} A &= \{1, 2, 3\} \\ B &= \{3, 4, 5\} \\ A - B &= \{1, 2, \} \end{aligned} \tag{0.13}$$

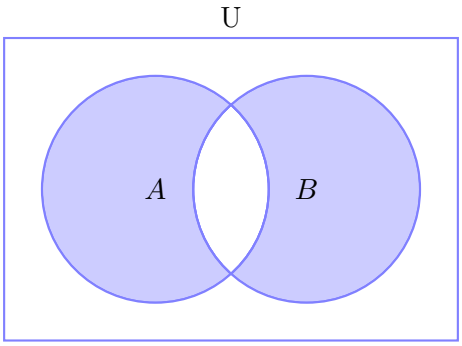
2. Membership Table ($A - B$)

A	B	$A - B$
0	0	0
0	1	0
1	0	1
1	1	0

Symmetric Difference ($\oplus$)

Definition 8 (Symmetric Difference)**.** *Given two sets A and B, the symmetric difference of A and B, $A \oplus B$, contains all the elements that are in A or in B* ***but not*** *in both.*

$$A \oplus B = \{x \mid (x \in A \text{ or } x \in B) \text{ and } x \notin A \cap B\} \tag{0.14}$$



1. Example

$$\begin{aligned} A &= \{1, 2, 3\} \\ B &= \{3, 4, 5\} \\ A \oplus B &= \{1, 2, 4, 5\} \end{aligned} \tag{0.15}$$

2. Membership Table ($A \oplus B$)

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

Summary

1. Operations

$$\begin{aligned} A &= \{1,2,3\} \\ B &= \{3,4,5\} \\ A \cup B &= \{1,2,3,4,5\} \\ A \cap B &= \{3\} \\ A - B &= \{1,2\} \\ A \oplus B &= \{1,2,4,5\} \end{aligned} \tag{0.16}$$

2. Membership Table

A	B	$A \cup B$	$A \cap B$	$A - B$	$A \oplus B$
0	0	0	0	0	0
0	1	1	0	0	1
1	0	1	0	1	1
1	1	1	1	0	0

Week 2

Learning objectives:

- Understand the concept of Venn diagrams and how they are used to represent and compare different set expressions.
- Understand and prove De Morgan's law using membership tables.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.128–137.
- Exercises

  pp.138–139 exercises 1–9, 14, 15, 17, 18, 22–26, 32 and 34–36.

1.201 The representation of a set using Venn diagrams

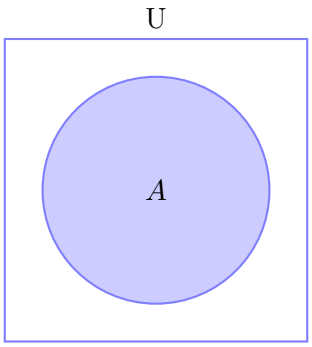
Venn diagrams can be used to represent sets and visualize the possible relations among a collection of sets. During this lesson we studied the following concepts:

- The universal set
- The complement of a set
- Set representation using Venn Diagrams

The Universal Set

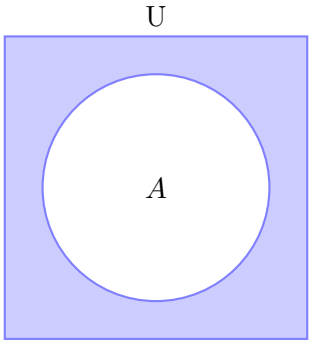
The universal set is a set containing everything. It's referred to by the letter `U`.

Note that $A \subseteq U$.



Complement of a set

Given a set A, the complement of A is written as $\overline{A}$, contains all the ements in the universal set U but not in A. It's represented by the area in red in figure below.



In other words $\overline{A} = U - A$.

Example

$$\begin{aligned} U &= \{1,2,3,4,5,6,7,8,9,10\} \\ A &= \{2,4,6,8,10\} \\ \overline{A} &= U - A \\ &= \{1,2,3,4,5,6,7,8,9,10\} - \{2,4,6,8,10\} \\ &= \{1,3,5,7,9\} \end{aligned} \tag{0.1}$$

The union of a set A with its completement $\overline{A}$ is always the universal set U.

$$A \cup \overline{A} = U \tag{0.2}$$

The symmetric difference of A and B is the same as the union of A and B minus the intersection of A and B:

$$A \oplus B = A \cup B - (A \cap B) \tag{0.3}$$

1.203 De Morgan's laws

De Morgan's laws describe how mathematical statements and concepts are related through their opposites. In se theory, they relate to intersection and unions of sets through their complements.

De Morgan's First Law

The complement of the union of two sets A and B is equal to the intersection of their complements.

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \tag{0.4}$$

De Morgan's Second Law

The complement of the intersection of two sets A and B is equal to the union of their complements.

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{0.5}$$

Proof using membership tables

1. $\overline{A \cup B} = \overline{A} \cap \overline{B}$

A	B	$\overline{A}$	$\overline{B}$	$A \cup B$	$\overline{A \cup B}$	$\overline{A} \cap \overline{B}$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

2. $\overline{A \cap B} = \overline{A} \cup \overline{B}$

A	B	$\overline{A}$	$\overline{B}$	$A \cap B$	$\overline{A \cap B}$	$\overline{A} \cup \overline{B}$
0	0	1	1	0	1	1
0	1	1	0	0	1	1
1	0	0	1	0	1	1
1	1	0	0	1	0	0

1.205 Laws of sets: Commutative, associative and distributive

We discussed three set identities: *Commutativity*, *Associativity*, and *Distributivity*.

Commutativity

When the order of operands in an operation does **NOT** affect the result, we say the operation is *commutative*. For example, addition is commutative

$$2 + 3 = 3 + 2 \tag{0.6}$$

Same applies for multiplication:

$$2 \cdot 3 = 3 \cdot 2 \tag{0.7}$$

Subtraction, however, is **NOT** commutative:

$$2 - 3 \neq 3 - 2 \tag{0.8}$$

In Set Theory, *Union* $\cup$, *Intersection* $\cap$, and *Symmetric Difference* $\oplus$ are all commutative operations. Much like in Algebra, Set difference is **NOT** commutative:

$$\begin{aligned} A &= \{1, 2\} \\ B &= \{1, 3\} \\ A - B &= \{1, 2\} - \{1, 3\} = \{2\} \\ B - A &= \{1, 3\} - \{1, 2\} = \{3\} \\ (A - B) &\neq (B - A) \end{aligned} \tag{0.9}$$

Associativity

When the grouping of elements in an operation doesn't change the result, we say the result is associative. Addition is associative:

$$(a + b) + c = a + (b + c) \tag{0.10}$$

In set theory, *Union*, *Intersection* and *Symmetric Difference* are all associative operations. Set difference is **not** associative:

$$\begin{aligned} A &= \{1,2\} \\ B &= \{1,3\} \\ C &= \{2,3\} \\ (A-B)-C &= (\{1,2\}-\{1,3\})-\{2,3\} \\ &= \{2\}-\{2,3\} \\ &= \emptyset \end{aligned} \tag{0.11}$$

$$\begin{aligned} A-(B-C) &= \{1,2\}-(\{1,3\}-\{2,3\}) \\ &= \{1,2\}-\{1\} \\ &= \{2\} \end{aligned}$$

$$\therefore (A-B)-C \neq A-(B-C)$$

Distributivity

The distributive property, in general, refers to the distributive law of multiplication which states that multiplying a sum of two numbers b and c by a coefficient a is the same as multiplying each addend by the coeficient a and adding the resulting products. We say the multiplication is distributive over the addition:

$$a \cdot (b+c) = a \cdot b + a \cdot c \tag{0.12}$$

Similarly, the set union is distributive over set intersection:

$$A \cup (B \cap C) = (A \cup B) \cap (B \cup C) \tag{0.13}$$

And the set intersection is distributive over the set union:

$$A \cap (B \cup C) = (A \cap B) \cup (B \cap C) \tag{0.14}$$

Table of Set Identities

Union	Name	Intersection
$A \cup B = B \cup A$	commutative	$A \cap B = B \cap A$
$(A \cup B) \cup C = A \cup (B \cup C)$	associative	$(A \cap B) \cap C = A \cap (B \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributive	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's Laws	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
$A \cup \emptyset = A$	identities	$A \cap \emptyset = \emptyset$
$A \cup U = U$		$A \cap U = A$
$A \cup \overline{A} = U$	complement	$A \cap \overline{A} = \emptyset$
$\overline{U} = \emptyset$		$\overline{\emptyset} = U$
$\overline{\overline{A}} = A$	double complement	
$A \cup (A \cap B) = A$	absorption	$A \cap (A \cup B) = A$
$A - B = A \cap \overline{B}$	set difference	

Applying set identities to simplify expressions

Show that $\overline{(A \cap B) \cup \overline{B}} = B \cap \overline{A}$

$$\begin{aligned}
\overline{(A \cap B) \cup \overline{B}} &= \overline{(A \cap B)} \cap \overline{\overline{B}} \\
&= \overline{(A \cap B)} \cap B \\
&= (\overline{A} \cup \overline{B}) \cap B \\
&= \overline{A} \cap B \cup \overline{B} \cap B \\
&= \overline{A} \cap B \cup \emptyset \\
&= \overline{A} \cap B \\
&= B \cap \overline{A}
\end{aligned} \tag{0.15}$$

1.207 Partition

A partition of an object is a subdivision of the object into parts such that the parts are completely separated from each other, yet together they form the whole object.

Data partitioning has many applications in Computer Science such as Big Data analysis. This is usually referred to as *Divide and Conquer* approach. Such techniques must be applied in cases where the entire input data doesn't fit into the physical memory of the Computer. In such cases, we must find a way to partition the data so that subsets of the original data can be operated on without changing the result of the whole computation.

Definition of a partition of a set

Two sets A and B are said to be disjointed if and only if $A \cap B = \emptyset$.

Definition 9 (Set Partition)**.** *A partition of set A is a set of subsets A_i such that all subsets are disjointed and then union of all subsets A_i is equal to A.*

Week 3

Learning objectives:

- Define a function.
- Describe the properties of functions.
- Explain how to plot a function.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.140–146.
- Exercises

  pp.153–154 exercises 1–4 and 6–17.

2.101 Introduction

A function is a rule that relates to how one quantity depends on another quantity. Much like a voltage depends on electrical current and resistance.

During this lecture, we learn the definition of a function and study a few of their properties.

2.102 The Definition of A Function

A function is a relation between a set of inputs and a set of outputs such that each input maps to exactly **one** output.

Definition

A function maps an element of set 1 to an element in set 2. Such mapping is *well-behaved* meaning that given a starting point we always know exactly where to go. For example, we could have a function that maps a set of strings to their corresponding number of characters:

$$
\begin{aligned}
S_1 &= \{Sea, Land, Sky\} \\
S_2 &= \{1, 2, 3, 4, 5, 6\}
\end{aligned}
$$

$$
\begin{aligned}
Sea &\to 3 \\
Land &\to 4 \\
Sky &\to 3
\end{aligned}
\tag{0.1}
$$

From Rosen's book, functions are defined as:

Definition 10 (Function)**.** *Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f : A \to B$ and read as f maps A to B.*

$x \in A : x \to f(x) = y \, (y \in B)$

Domain, co-domain and range of a function

Given a function $f : A \to B$

$x \in A \to f(x) = y \in B$

A is the set of inputs and its referred to as the *Domain of f*. We write it as $D_f = A$.

B is the set containing all possible outputs; referred to as the *co-domain of f*. We write it as $co - D_f = B$.

The set containing all outputs is called the *Range of f* and is written as R_f.

Image and pre-image (antecedent) of an element

y, the output of the function of a given input x, is called the *Image of x* where x itself is called the *pre-image of y*. We write $f(x) = y$.

Example of Domain, co-domain and range

Let A be the set $\{On, Sea, Land, Sky\}$, B be the set $\{1, 2, 3, 4, 5, 6\}$, and f be the function that maps the set of strings to their corresponding number of characters. We have:

$$
\begin{aligned}
On &\to 2 \\
Sea &\to 3 \\
Land &\to 4 \\
Sky &\to 3
\end{aligned}
\tag{0.2}
$$

In this case:

$$\begin{aligned} D_f &= A = \{On, Sea, Land, Sky\} \\ co-D_f &= B = \{1, 2, 3, 4, 5, 6\} \\ R_f &= \{2, 3, 4\} \end{aligned} \tag{0.3}$$

Moreover, we can say that 2 is the image of the string *On* and *On* is the pre-image of 2. $Pre - images(2) = \{On\}$.

3 is the image of *Sea* and *Sky*, therefore $Pre - images(3) = \{Sea, Sky\}$.

2.104 Plotting functions

We explore and plot some special functions.

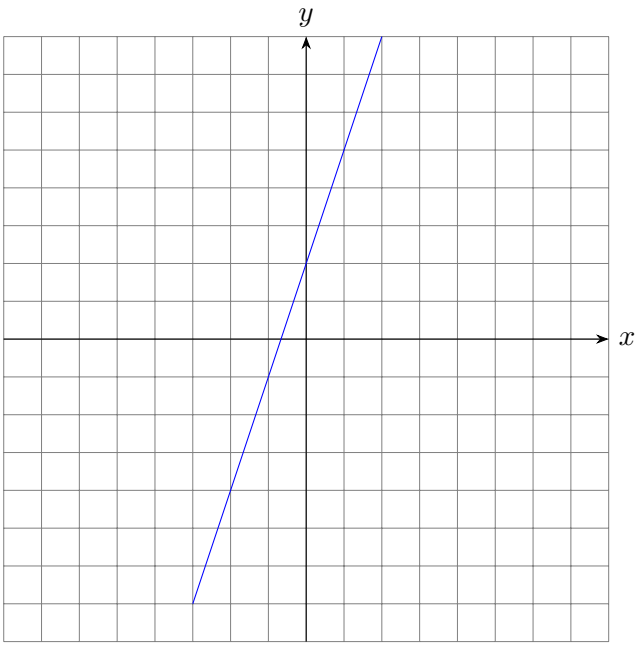
Linear Functions

A function f is called a linear function if it is of the form $f(x) = ax + b$. This function is a straight line passing through the point $(0, b)$ with gradient a.

If $a > 0$, then the function is increasing. It's decreasing if $a < 0$.

In order to plot this function, first we make a table of values for this function. We use $f(x) = 3x + 2$ as an example.

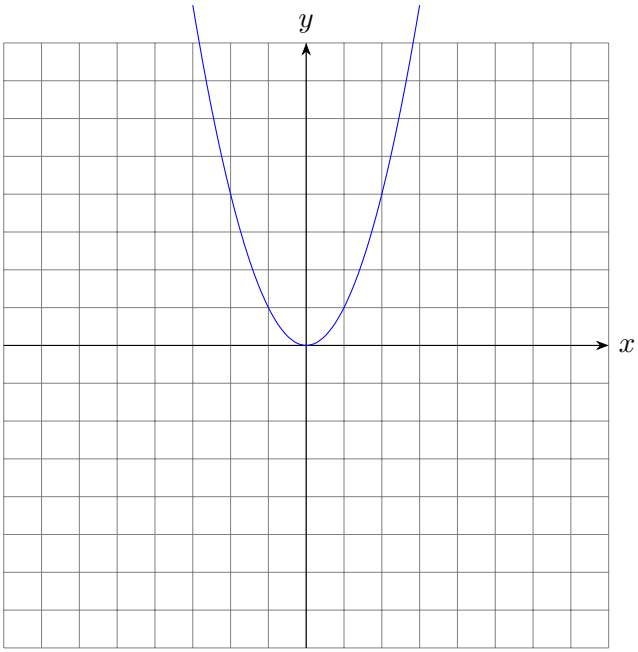
x	f(x)
0	2
1	5
2	8
3	11
4	14



Quadratic functions

A function f of the form $f(x) = ax^2 + bx + c$ is called a *Quadratic function.*

x	f(x)
0	0
1	1
2	4
3	9
4	16



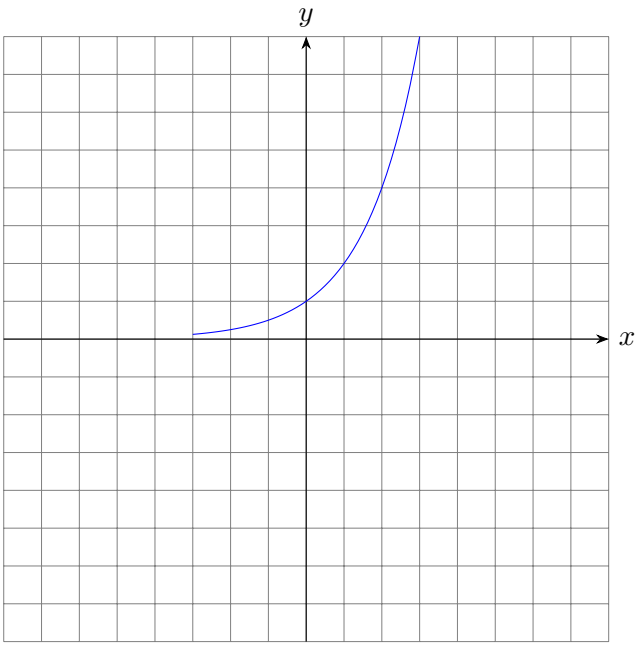
Exponential functions

A function f of the form $f(X) = b^x$ is called an *exponential function*. The variable b is called the *base* of the function.

A more formal definition may be:

Definition 11 (Exponential Function)**.** *The function f defined by $f : \mathbb{R} \to \mathbb{R}^+$ and $f(x) = b^x$ where $b > 0$ and $b \neq 1$ is called and exponential function with a base b.*

x	f(x)
0	1
1	2
2	4
3	8
4	16



Exponentials have some properties which are good to remember:

Form	Result
$b^x \cdot b^y$	b^{x+y}
$\frac{b^x}{b^y}$	b^{x-y}
$(b^x)^y$	$b^{x \cdot y}$
$(a \cdot b)^x$	$a^x \cdot b^x$
$\left(\frac{a}{b}\right)^x$	$\frac{a^x}{b^x}$
b^{-x}	$\frac{1}{b^x}$

The point $(0, 1)$ is the common point for all exponentials. When $b > 1$ we have an exponential growth. When $0 < b < 1$, we have exponential decay.

2.106 Injective and surjective functions

Injective Functions

Let $f : A \to B$ be a function; f is said to be injective, or *one-to-one* if and only if $\forall a, b \in A$, if $a \neq b$ then $f(a) \neq f(b)$. In plain english, this means that two different inputs will lead to two different outputs, i.e. given two different inputs a and b, then the **image** of a is different than the image of b.

A corollary of this is that:

Corollary 1. $\forall a, b \in A, f(a) = f(b) \to a = b$

1. Example: linear function

Show that a function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 3$ is an injection (one-to-one).

We can prove this in two different ways. The first proof assumes $f(a) = f(b)$

Proof. Let $a, b \in \mathbb{R}$, show that if $f(a) = f(b)$ then $a = b$.

$$\begin{aligned} f(a) = f(b) \to & 2a + 3 = 2b + 3 \\ & 2a + 3 - 3 = 2b + 3 - 3 \\ & 2a = 2b \\ & \frac{2a}{2} = \frac{2b}{2} \\ & a = b \end{aligned} \tag{0.4}$$

$\therefore f$ is injective. □

The second proof assumes $a \neq b$

Proof. Let $a, b \in \mathbb{R}$, show that if $a \neq b$ then $f(a) \neq f(b)$.

$$\begin{aligned} a \neq b \to & 2a \neq 2b \\ & 2a + 3 \neq 2b + 3 \\ & f(a) \neq f(b) \end{aligned} \tag{0.5}$$

$\therefore f$ is injective. □

2. Example: quadratic function

To prove that a function is not injective, we only need to find one example of two different inputs having the same image.

Show that a function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ is not injective.

Proof.

$$\begin{aligned} & f(5) = (5)^2 = (-5)^2 = f(-5) \\ & \text{however } 5 \neq -5 \end{aligned} \tag{0.6}$$

$\therefore f$ is not injective. □

However, if we change the domain of the function such that $f : \mathbb{R}^+ \to \mathbb{R}$, we can make it injective. To prove this, we can apply the same two methodologies from the previous example.

Surjective Functions

Let $f : A \to B$ be a function; f is said to be surjective, or *onto* if and only if $\forall y \in B \, \exists x \in A \mid y = f(x)$. This means that every element in the co-domain of f, B, has **at least** one pre-image in the domain of f, A. This is equivalent to saying that the range and the co-domain of a surjective function, are equal (i.e. $R_f = co - D_f$).

1. Example: linear function

   Show that a function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 3$ is a surjection (onto).

   To prove this, we must show that for every element in B, there is a pre-image in A.

   Proof. Let $y \in \mathbb{R}$, show that $\exists x \in \mathbb{R} \mid f(x) = y$.

   $$\begin{aligned} f(x) = y \to & 2x + 3 = y \\ & 2x + 3 - 3 = y - 3 \\ & \frac{2x}{2} = \frac{y-3}{2} \\ & x = \frac{y-3}{2} \in \mathbb{R} \end{aligned} \tag{0.7}$$

   $\therefore \forall y \in \mathbb{R} \exists x = \frac{y-3}{2} \in \mathbb{R} \mid f(x) = y$, hence f is surjective. □

2. Example: quadratic function

   Show that a function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = x^2$ is not a surjection.

   Proof. Let $y \in \mathbb{R}$, show that $\exists x \in \mathbb{R} \mid f(x) = y$.

   Let $y \in \mathbb{R}$, show that $\exists x \in \mathbb{R} \mid f(x) = y$.

   $R_f = [0, +\infty[\neq co - D_f = \mathbb{R}$

   $\therefore f$ is not surjective. □

Week 4

Learning objectives:

- Discuss special functions.
- Describe inverse functions.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.146–153.
- Exercises

  pp.153–155 exercises 5, 14–25, 30–36, 44–46 and 49.

For logarithmic and exponential functions, please read Appendix 2 and complete exercises 1 to 6 in Appendix 2.

2.201 Function composition

Using examples we will understand function composition and how to work out the composition of two functions. We will also show that function composition is **not** commutative.

Given two functions, f and g, the composition of f and g is written as $f \circ g = f(g(x))$.

For example, let $f(x) = 2x$ and $g(x) = x^2$, the composition of f and g can be worked out as follows:

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f(x^2) \\ &= 2x^2\end{aligned}$$

$$\begin{aligned}(f \circ g)(1) &= f(g(x)) \\ &= f(1^2) \\ &= 2 \cdot 1^2 \\ &= 2\end{aligned}$$

What this means is that if we have a function $g : A \to B$ and a function $f : B \to C$, function composition allows us to produce a function $(f \circ g) : A \to C$.

Note that function composition is **not** commutative. In other words, $f \circ g \neq g \circ f$. Let $f = 2x$ and $g = x^2$, we can show that $(f \circ g) = 2x^2$ and $(g \circ f) = 4x^2$.

2.203 Bijective functions

Definition

A bijective or invertible function is a function $f : A \to B$ that can be described as both *injective* and *surjective* simultaneously. This means that each element of the *co-domain* has exactly one *pre-image*.

Definition 12 (Bijection)**.** *A function $f(x)$ is said to be bijective if and only if it is both injective and surjective.*

Exercise 1:

Show that the function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 3$ is a bijective (invertible) function.

Proof. To prove this, suffices to prove that this function is both an injection and a surjection. Let's prove the injection case first:

Let $a, b \in \mathbb{R}$, we will show that if $f(a) = f(b)$ then $a = b$.

$$\begin{aligned} f(a) = f(b) \to & 2a + 3 = 2b + 3 \\ & 2a + 3 - 3 = 2b + 3 - 3 \\ & 2a = 2b \\ & \frac{2a}{2} = \frac{2b}{2} \\ & a = b \end{aligned}$$

$\therefore f$ is injective.

Now turning our attention to the surjection case, we have:

Let $y \in \mathbb{R}$, we will show that $\forall y \in \mathbb{R} \exists x \in \mathbb{R} \mid f(x) = y$.

$$\begin{aligned} f(x) = y \to & 2x + 3 = y \\ & 2x + 3 - 3 = y - 3 \\ & \frac{2x}{2} = \frac{y - 3}{2} \\ & x = \frac{y - 3}{2} \in \mathbb{R} \end{aligned}$$

$\therefore \forall y \in \mathbb{R} \exists x = \frac{y-3}{2} \in \mathbb{R} \mid f(x) = y$, hence f is surjective.

Because we have proved that $f(x) = 2x + 3$ is both an injection and a surjection, we have also proved that it is a bijection. □

Inverse function

Definition 13 (Inverse function)**.** *Let $f : A \to B$, if f is bijective, then the inverse function f^{-1} exists and is defined as $f^{-1} : B \to A$.*

Given this definition, let's find the inverse of $2x + 3$.

Exercise 2:

The following function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 3$ is a bijection. Find the inverse function f^{-1}.

$$\begin{aligned} f(x) &= 2x + 3 \\ f(x) &= y \\ 2x + 3 &= y \\ 2x + 3 - 3 &= y - 3 \\ \frac{2x}{2} &= \frac{y-3}{2} \\ x &= \frac{y-3}{2} \end{aligned}$$

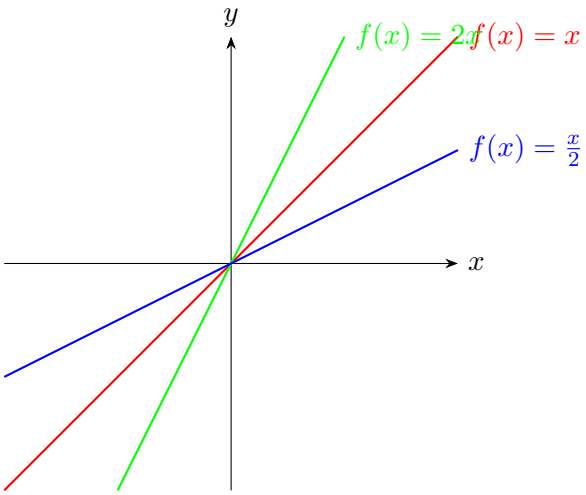
$$\therefore f^{-1}(x) = \frac{x-3}{2}$$

Identity function

There is one special case of composition which is $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x$. For example if $f(x) = 2x$, then $f^{-1}(x) = \frac{x}{2}$, therefore $(f \circ f^{-1})(x) = 2\frac{x}{2} = x$. Similarly, $(f^{-1} \circ f)(x) = \frac{2x}{2} = x$.

Plotting the inverse function

The function f and its inverse f^{-1} are always symmetric to the straight line $y = x$.



2.205 Logarithmic functions

Exponential and logarithmic functions are closely related. Therfore, let's review exponential functions before dealing with logarithmic functions.

Exponential functions were defined back in Definition 11. We know from that definition that:

$$y = f(x) = b^x \ (b > 0, \ b \neg 1)$$

The domain of the function is $(-\infty, +\infty)$.

The range of the function is $(0, +\infty)$.

The graph of an exponential function **always** passes through the point with coordinates $(0, 1)$. If the base b is greater than 1, then the function is increasing on $(-\infty, +\infty)$ and we call it *exponential growth*. Conversely, if $b < 1$, then the function is decreasing on $(-\infty, +\infty)$ and we call it *exponential decay*.

Definition

With that review out of the way, we can define Logarithmic functions:

Definition 14 (Logarithmic function)**.** *The logarithmic function with base b where $b > 0$ and $b \neq 1$ is defined as follows:*

$$log_b x = y \leftrightarrow x = b^y$$

We can say that $log_b x$ is the inverse function of the exponential function b^x.

Laws of logarithmic functions

1. $log_b m \times n = log_b m + log_b n$
2. $log_b \frac{m}{n} = log_b m - log_b n$
3. $log_b m^n = n\ timeslog_b m$
4. $log_b 1 = 0$
5. $log_b b = 1$

Exercise 1

1. $log_3 81$

   $log_3 81 = log_3 3^4 = 4 \times log_3 3 = 4 \times 1 = 4$

2. $log_{10} 100$

   $log_{10} 100 = log_{10} 10^2 = 2 \times log_{10} 10 = 2 \times 1 = 2$

3. $log_3 \frac{1}{81}$

   $log_3 \frac{1}{81} = log_3 81^{-1} = log_3 3^{-4} = -4 \times log_3 3 = -4 \times 1 = -4$

4. $log_2 1$

   $log_2 1 = log_2 2^0 = 0 \times log_2 2 = 0 \times 1 = 0$

Natural logarithm

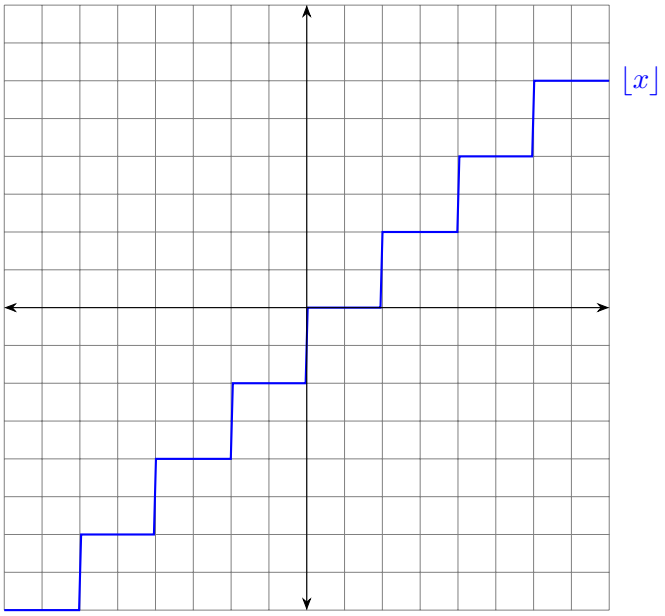
The natural logarithm, commonly written as $ln(x)$ is the logarithm with base e. In other words: $ln(x) = log_e x$ where $e \approx 2.71828$.

2.207 Floor and ceiling functions

Floor function

Definition 15 (Floor function)**.** *The **floor** function is a function $f : \mathbb{R} \to \mathbb{Z}$. It takes a real number x as input and outputs the largest integer that is less than or equal to x. Denoted as $floor(x) = \lfloor x \rfloor$.*

For example, given a real number x such that $n \leq x < n+1$, the floor of x is n. In other words: $floor(x) = \lfloor x \rfloor = n$.

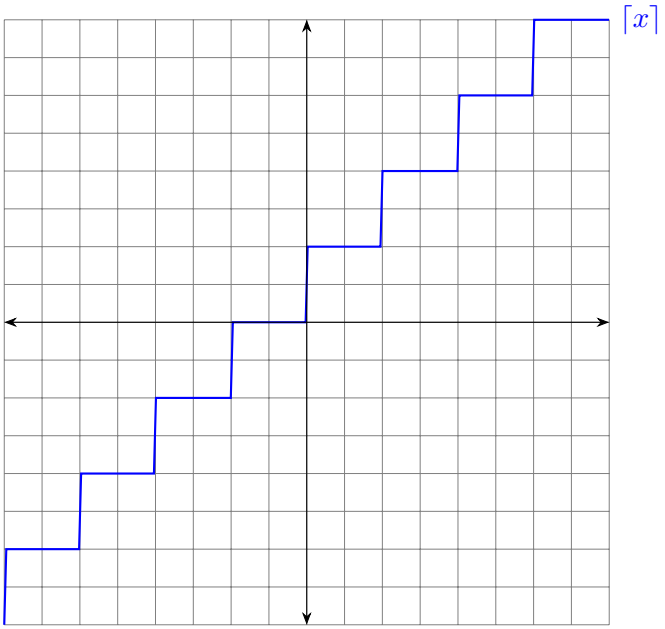


We can think of the floor function as if we're walking on the number line to the left until we find an integer. This means that $\lfloor 1.1 \rfloor = 1$ but $\lfloor -1.1 \rfloor = -2$.

Ceiling function

Definition 16 (Ceiling function)**.** *The* ***ceiling*** *function is a function* $f : \mathbb{R} \to \mathbb{Z}$*. It takes a real number* x *as input and outputs the smallest integer that is greater than or equal to* x*. Denoted as* $ceiling(x) = \lceil x \rceil$*.*

For example, given a real number x such that $n < x \leq n+1$, the ceiling of x is $n+1$. In other words: $ceiling(x) = \lceil x \rceil = n + 1$.



This is exact opposite of the floor function. So we can think of it as if were were walking on the number line to the right until we find an integer. This means that $\lfloor 1.1 \rfloor = 2$, but $\lfloor -1.1 \rfloor = -1$.

Exercise 1

Let n be an integer and x a real number. Show that:

$$\lfloor x + n \rfloor = \lfloor x \rfloor + n$$

Proof. Let m be an integer such that $m = \lfloor x \rfloor$. By definition of the floor function we have $m \leq x < m+1$. Addin n to both sides of this inequality, we have $m+n \leq x+n < m+n+1$.

This implies that $\lfloor x + n \rfloor = m + n$ by definition. And $m = \lfloor x \rfloor$. Therefore $\lfloor x + n \rfloor = \lfloor x \rfloor + n$. □

Week 5

Learning Objectives

- Explain and apply basic concepts of propositional logic.
- Construct truth tables of propositions and use them to demonstrate the equivalence of logical statements.
- Translate natural language statements into symbolic logical statements and vice versa.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.1–12.
- Exercises

  p.12 exercises 1–3.

3.101 Introduction to propositional logic

Definition 17 (Propositional Logic)**.** *It is a branch of logic that is interested in studying mathematical statements.*

Propositional Logic is the basis of all mathematical reasoning and the rules used to construct mathematical theories. Its original purpose was to model reasoning and dates back to Aristotle.

Effectively, it is an *algebra of propositions*. In this *algebra*, the variables are unknown **propositions** rather than unknown **real numbers**.

The operators used are and ($\wedge$), or ($\vee$), not ($\neg$), implies ($\rightarrow$) and if and only if ($\leftrightarrow$) instead of our regular $+$, $-$, $\times$, and $\div$.

Applications of propositional logic

Propositional logic can be used in logic circuit design. It can also be applied to programming languages, such as Prolog.

Many computer reasoning systems, including theorem provers, program verifiers and applications in the field of Artificial Intelligence, have been implemented in logic-based programming languages.

These languages, generally employ predicate logic, a form of logic that extends the capabilities of propositional logic.

3.103 Propositions

Definition 18 (Proposition)**.** *A declarative sentence that is either true or false, but not both.*

A Proposition is the most basic element of logic. Which means that propositions are the building blocks for our reasoning and logical statements.

Examples of propositions

As mentioned above, a proposition must be a declarative statement that is either true or false, therefore the following statements are propositions:

- **London is the capital of the United Kingdom**

  We know this is true, so this is considered to be a **true proposition**.

- $\mathbf{1 + 1 = 2}$

  This is also a **true proposition**.

- $\mathbf{2 < 3}$

  This is also a **true proposition**.

- **Madrid is the capital of France**

  This is a **false proposition**.

- $\mathbf{3 < 2}$

  This is also a **false proposition**.

- **10 is an odd number**

  This is also a **false proposition**.

What follows is a series of statements which are **not** propositions, as they can not assume a true or false value:

- $x + 1 = 2$

  We don't know the value of x, so this is **not** a proposition. However, if a value is assigned to x, then at that moment it becomes a proposition. IF we assign the

value 1 to x, this will be a **true** proposition, if any other value is assigned to x, then it'll be a **false** proposition.

- $x + y = z$

  Also not a proposition as x, y and z have no values.

- What time is it?

  Is not a proposition as it is not a declarative sentence.

Propositional Variables

To avoid writing long, repetivive propositions, we make use of **propositional variables**. They are typically a letter, such as **p**, **q**, **r**, ...

We can assign letters to our previous propositions, for example: Let p be the proposition *London is the capital of the United Kingdom.*

3.105 Truth tables and truth sets

As we begin to build more complex compound propositions, we need a method of keeping track of this proposition's truth value. A truth table is one such method.

True Tables

A truth table is tabular representation of all the possible combinations of truth values for a set of propositional variables.

For example:

p	q
F	F
F	T
T	F
T	T

A truth table of n propositional variables, will contain 2^n rows. So a table for 3 propositional variables, will have 8 rows:

p	q	r
F	F	F
F	F	T
F	T	F
F	T	T
T	F	F
T	F	T
T	T	F
T	T	T

Truth Set

Definition 19 (Truth Set)**.** *Let p be a proposition on a set S. The truth set of p is the set of elements of S for which p is true.*

Commonly, we use a capital letter to refer to the truth set of a proposition. For example the truth set of a proposition p is referred to as P.

1. Example

   Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

   Let p and q be two propositions concerning an integer n in S, defined as follows:

   $p : n$ is even
   $q : n$ is odd

   Therefore, the truth set of p is $P = \{2, 4, 6, 8, 10\}$ and the truth set of q is $Q = \{1, 3, 5, 7, 9\}$.

3.107 Compound propositions

Compound propositions are built by combining propositions with logical operators (also referred to as connectives). The connectives which we deal with in this lecture are:

- **Negation** $\neg$
- **Conjunction** $\wedge$
- **Disjunction** $\vee$
- **Exclusive-or** $\oplus$

Negation $\neg$

Let p be a proposition, the negation of p, denoted by $\neg p$, and read as "not p", is the statement: *it is **not** the case that p.*

For example if p is the statement *John's program is written in Python*, then $\neg p$ is the statement *John's program is* ***not*** *written in Python.*

p	$\neg p$
F	T
T	F

Conjunction $\wedge$

Let p and q be propositions, the conjuntion of p and q, denoted by $p \wedge q$, and read as "p and q", is the statement: *p and q.*

The conjunction is only true when both p and q are true and false otherwise.

For example if p is the statement *John's program is written in Python*, and q is the statement *John's program has less then 20 lines of code*, then $p \wedge q$ is the statement *John's program is written in Python* ***and*** *has less than 20 lines of code.*

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

Disjunction $\vee$

Let p and q be propositions, the disjuntion of p and q, denoted by $p \vee q$, and read as "p or q", is the statement: *p or q.*

The disjunction is only false when both p and q are false and true otherwise.

For example if p is the statement *John's program is written in Python*, and q is the statement *John's program has less then 20 lines of code*, then $p \vee q$ is the statement *John's program is written in Python* ***or*** *has less than 20 lines of code.*

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

Exclusive-or $\oplus$

Let p and q be propositions, the exclusive-or of p and q, denoted by $p \oplus q$, and read as "p exclusive-or q", is the statement: *p exclusive-or q.*

The exclusive is true when either p or q are true, but not both.

For example if p is the statement *John's program is written in Python*, and q is the statement *John's program has less then 20 lines of code*, then $p \oplus q$ is the statement *John's program is written in Python* ***or*** *has less than 20 lines of code,* ***but not both****.*

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Precedence of logical operators

Propositions can be combined to build complex compound propositions. To do this we need to start relying on precedence of logical operators or use parenthesis.

The meaning of compound propositions can change depending on the order in which parentheses are used. For example $(p \vee q) \wedge (\neg r) \neq p \vee (q \wedge \neg r)$.

Here's a small table of precedence:

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3

Exercise

Given a positive integer n, let's consider the propositions p and q, where:

- p: *n is an even number*
- q: *n is less than 10*

Let's write the logical expression for each of the following propositions:

1. *n is an even number* **and** *is less than 10* $p \wedge q$
2. *n is either an even number* **or** *is less than 10* $p \vee q$
3. *n is either an even number* **or** *is less than 10* **but not both** $p \oplus q$
4. $\neg p \vee (p \wedge q)$

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$\neg p$	$\neg p \vee (p \wedge q)$
F	F	F	F	F	T	T
F	T	F	T	T	T	T
T	F	F	T	T	F	F
T	T	T	T	F	F	T

Week 6

Learning Objectives

- How to formalise a logical implication
- Apply the laws of propositional to analyse propositions and arguments.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.1–12.
- Exercises

  p.13 exercises 6–12

  p.14 exercises 19–21

  p.33 exercises 6–11.

3.202 Logical implication ($\rightarrow$)

Definition 20 (Implication)**.** *Let p and q be propositions. The conditional statement or implication $p \rightarrow q$ is the proposition "if p then q".*

p is called the hypothesis (or antecedent) q is called the conclusion (or consequence)

1. Example 1

   Let p and q be the following statements:

   - p: John did well in Discrete Mathematics
   - q: John will do well in the Programming Course

   The conditional statement $p \rightarrow q$ can be written as follows:

   If John did well in Discrete Mathematics then John will do well in the Programming Course.

Truth Table

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

As we can see, the only situation where an implication evaluates to false is when our hypothesis is true but the conclusion is false.

Different expressions for $p \to q$

Let p and q be the following statements:

- p: It's sunny
- q: John goes to the park

There are many ways to write the conditional statement $p \to q$:

- $p \to q$
- if p **then** q
- if p, q
- p implies q
- p only if q
- q follows from p
- p is sufficient for q
- q unless $\neg p$
- q is necessary for p

All of these forms are equivalent to *if it's sunny then John goes to the park.*

Note that the statement *John going to the park is necessary for a sunny day* sounds a bit strange in English. We should try to think of it as *John going to the park is a necessary consequence of a sunny day.*

Converse, inverse and contrapositive

Let p and q be propositions and A the conditional statement $p \to q$.

The conditional statement $q \to p$ is referred to as the **converse** of A.

The conditional statement $\neg q \to \neg p$ is referred to as the **contrapositive** of A.

The conditional statement $\neg p \to \neg q$ is referred to as the **inverse** of A.

The **contrapositive** of A has the same truth table as A and is, therefore, equivalent to it.

1. Example 2

   Let p and q be the following statements:

   - p: It's sunny
   - q: John goes to the park
   - $A = p \to q$: If it's sunny then John goes to the park

   Therefore:

   - **converse**: If John goes to the park, then it's sunny
   - **contrapositive**: If John does not go to the park, then it's not sunny
   - **inverse**: If it's not sunny then John does not go the park

   We can build a large truth table with all of these:

p	q	$p \to q$	$\neg q \to \neg p$	$\neg p \to \neg q$	$q \to p$
F	F	T	T	T	T
F	T	T	T	F	F
T	F	F	F	T	T
T	T	T	T	T	T

   Note, also, that the **converse** or A and the **inverse** of A are equivalent.

3.204 Logical equivalence ($\leftrightarrow$)

Definition 21 (Logical Equivalence)**.** *Let p and q be propositions. The **biconditional** or **equivalence** statement $p \leftrightarrow q$ is the proposition $p \to q \wedge q \to p$.*

Biconditional statements are also called bi-implications and can be read p ***if and only if*** q

Truth Table

p	q	$p \leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

We can see here that the biconditional statement of p and q is true whenever p and q have the same truth value and is false otherwise.

Equivalent propositions

Let p and q be propositions. We say that p and q are *logically equivalent* if they always have the same truth value.

We write $p \equiv q$ to signify that p is equivalent to q.

Note that $\equiv$ is not a logical operator, and $p \equiv q$ is not a compound proposition. $p \equiv q$ means that the compound proposition $p \leftrightarrow q$ is always true.

Proving equivalence

One way of determining logical equivalence, is by means of truth tables and verifying that two propositions have the same truth values for every possible input.

p	q	$p \to q$	$\neg p$	$\neg p \vee q$
F	F	T	T	T
F	T	T	T	T
T	F	F	F	F
T	T	T	F	T

If values difer in any row, then we demonstrate non-equivalence.

1. Example 1

   Let p, q, and r be the following propositions concerning n:

   - p: $n = 20$
   - q: n is even
   - r: n is positive

   Let's express each conditional statement below symbolically:

   - **If** $n = 20$, **then** n is positive

     $p \to r$

   - $n = 20$ **if** n is even

     $q \to p$

   - $n = 20$ **only if** n is even

     $p \to q$

Precedence of logical operators (Updated)

Propositions can be combined to build complex compound propositions. To do this we need to start relying on precedence of logical operators or use parenthesis.

The meaning of compound propositions can change depending on the order in which parentheses are used. For example $(p \vee q) \wedge (\neg r) \neq p \vee (q \wedge \neg r)$.

Here's a small table of precedence:

Operator	Name	Precedence
$\neg$	Negation	1
$\wedge$	Conjunction	2
$\vee$	Disjunction	3
$\rightarrow$	Conditional or Implication	4
$\leftrightarrow$	Biconditional or Equivalence	5

3.206 Laws of propositional logic

The following table summarizes the laws of Propositional Logic.

	Disjunction	Conjunction
Idempotent laws	$p \vee p \equiv p$	$p \wedge p \equiv p$
Commutative laws	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
Associative laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Distributive laws	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Identity laws	$p \vee \mathbf{F} \equiv p$	$p \wedge \mathbf{T} \equiv p$
Domination laws	$p \vee \mathbf{T} \equiv \mathbf{T}$	$p \wedge \mathbf{F} \equiv \mathbf{F}$
De Morgan's laws	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation laws	$p \vee \neg p \equiv \mathbf{T}$[1]	$p \wedge \neg p \equiv \mathbf{F}$[2]
Double negation law	$\neg\neg p \equiv p$	

[1] A statement that's always **true** is a *Tautology*
[2] A statement that's always **false** is a *Contradiction*

Week 7

Learning Objectives

- Describe the basic concepts of predicate logic.
- Describe existential and universal quantifiers.
- Assign truth values to quantified statements.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.34–49 and pp.53–60.
- Exercises

  pp.50–51 exercises 1–8, 10–12 and 15–20

  p.60 exercises 1–5.

4.101 Introduction to predicate logic

Our previous Propositional Logic is useful for studying propositions but has some limitations:

- It cannot express precisely the meaning of complex mathematical statements.
- It only studies propositions, i.e. statements with known truth values

Predicate Logic is a different type of Mathematical Logic which overcomes the limitations of Propositional Logic and can be used to build more complex reasoning.

Example 1

Given the statements:

- *All* ***men*** *are* ***mortal****.*
- ***Socrates*** *is a* ***man****.*

It's natural to conclude that *Socrates* is a *man*. This sort of reasoning cannot be expressed by Propositional Logic. Predicate Logic enables us to formalise it.

Example 2

Given the statement ***x** square is equal to **4***. We **know** this statement is **NOT** a proposition as its truth value is a function depending on **x**, however Predicate Logic can express and formalise this statement.

4.103 What are predicates?

We start with some examples of statements which cannot be expressed by Propositional Logic.

Insufficiency of Propositional Logic

Going back to the previous example ***x** squared is equal to **4***. We already saw that this statement cannot be a proposition because its truth value is a function depending on **x**.

Definition of Predicate

Predicates are generalizations of propositions. They are (Boolean) functions which return *TRUE* or *FALSE* depending on their variables. They **become** propositions when their variables are assigned values.

Predicates, much like regular sentences, are composed of smaller parts. The statement ***x** square is equal to **4*** contains two parts: the variable **x**; and the predicate **is equal to 4**.

We can formalize this statement as $P(x)$ where P is the predicate *squared is equal to 4* and x is the variable.

P is referred to as the *Propositional Function*.

As soon as a value is assigned to the variable x, the statement $P(x)$ becomes a proposition and has a truth value.

1. Example 1

   Let x be an integer and let P be the propositional function *square is equal to 4*, therefore $P(2)$ is *TRUE* and $P(3)$ is *FALSE*.

Predicates with multiple variables

It's important to note that Predicates can depend on **more than one** variable.

1. Example 1

   Let $P(x, y)$ denote $x^2 > y$, therefore $P(-2, 3) \equiv 4 > 3$ is *TRUE* and $P(2, 4) \equiv 4 > 4$ is *FALSE*.

2. Example 2

   Let $Q(x, y, z)$ denote $x + y < z$, therefore $Q(2, 4, 5) \equiv 2 + 4 < 5$ which is *FALSE*, $Q(1, 2, 4) \equiv 1 + 2 < 4$ which is *TRUE*, and $Q(1, 2, z)$ is **NOT** a proposition.

Logical operations

All logic previously defined for propositional logic carries over to predicate logic.

1. Example 1

   If $P(x)$ denotes $x^2 < 16$, then $P(1) \vee P(-5) \equiv (1 < 16) \vee (25 < 16) \equiv \mathbf{T} \vee \mathbf{F} \equiv \mathbf{T}$.

4.105 Quantification

Quantification expresses the extent to which a predicate is true over a range of elements.

The two most most important quantifiers are the universal quantifier $\forall$ and the existential quantifier $\exists$.

There is a third quantifier called the uniqueness quantifier $\exists!$.

1. Example 1

   The following statements give examples of **quantified predicates**.

   - *All men are mortal.*
   - *Some computers are not connected to the network.*

Universal Quantifier $\forall$

The Universal Quantification of a predicate $P(x)$ is the proposition:

- $P(x)$ is true for all values of x in the universe of discourse.

We use the notation $\forall x P(x)$ and read it as *for all x.*

If the universe of discourse is finite $\{n_1, n_2, \ldots, n_k\}$ then the universal quantifier is the **conjunction** of the propositions over all elements: $\forall x P(x) \equiv P(n_1) \wedge P(n_2) \wedge \ldots \wedge P(n_k)$.

1. Example 1

   Let P, Q denote the following propositional functions of x:

   - $P(X)$: x must take a discrete mathematics course
   - $Q(X)$: x is a Computer Science student

   Where the universe of discourse for both $P(x)$ and $Q(x)$ is all university students. Let's express the following statements symbolically:

- Every CS student must take a course on discrete mathematics.

  $\forall x Q(x) \rightarrow P(x)$

- Everybody must take a discrete mathematics course or be a CS student.

  $\forall x (P(x) \vee Q(x))$

- Everybody must take a discrete mathematics course and be a CS student.

  $\forall x (P(x) \wedge Q(x))$

2. Example 2

   Let's formalise the following statement S

   - S: For every x and for every y, $x + y > 10$

     Let $P(x, y)$ be the statement $x + y > 10$, where the universe of discourse is the set of all integers.

     $\forall x \forall y P(x, y) \equiv \forall x, y P(x, y)$

Existential Quantifier $\exists$

The existential quantification of a predicate $P(x)$ is the proposition *There exists a value of x in the universe of discourse, such that $P(x)$ is true.*

If the universe of discourse is finite $\{n_1, n_2, \ldots, n_k\}$, then the existential quantifier is the **disjunction** of the proposition over all elements: $\exists x P(x) \equiv P(n_1) \vee P(n_2) \vee \ldots \vee P(n_k)$.

1. Example 1

   Let $P(x, y)$ denote the statement $x + y = 5$. The expression $\exists x \exists y P(x, y)$ means "There exists a value x and a value y in the universe of discourse such that $x+y = 5$ is true".

2. Example 2

   Let a, b, c denote fixed real numbers and S be the statement /There exists a real solution to $ax^2 + bx - c = 0$. S can be expressed as $\exists x P(x)$.

Uniqueness Quantifier $\exists!$

The uniqueness quantification of a predicate $P(x)$ is the proposition *There exists a unique value x in the universe of discourse such that $P(x)$ is true.*

The uniqueness quantifier is a **special case** of the existential quantifier.

We use the notation $\exists! x P(x)$ and read it as /there exists a unique x".

Example 1

Let $P(x)$ be the statement $x^2 = 4$. The expression $\exists! x P(x)$ means "There exists a unique value of x such that $x^2 = 4$ is true".

4.107 Nested Quantifiers

When we want to express statements with multiple variables, we employ nested quantifiers.

Nested Quantifier	Meaning
$\forall x \forall y P(x, y)$	$P(x, y)$ is true for every pair (x, y)
$\exists x \exists y P(x, y)$	There is a pair (x, y) for which $P(x,y) is true
$\forall x \exists y P(x, y)$	For all x, there is a y for which P(x,y) is true
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for all y

Binding Variables

A variable is said to be **bound** if it is within the scope of a quantifier. A variable that is **not bound** is called a **free** variable.

1. Example 1

   Let P be a propositional function and S be the statement $\exists x P(x, y)$. In this case, x is **bound** while y is **free**.

Logical operations

All the logical operations discussed previously, can also be applied to quantified statements.

Order of operations

When we have quantifiers of the same type, either all universal or all existential, the other doesn't matter. However, when we're dealing with quantifiers of different types we **must** apply the quantifiers at the correct order.

1. Example 1

   $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$

   However

   $\forall x \exists y P(x, y) \neq \exists y \forall x P(x, y)$

Precedence of Quantifiers

The quantifiers $\forall$ and $\exists$ have precedence over **all** other logical operators. This means that $\forall x P(x) \vee Q(x)$ should be read as $(\forall x P(x)) \vee Q(x)$ and $\forall x P(x) \rightarrow Q(x)$ is to be read as $(\forall x P(x)) \rightarrow Q(x)$.

Week 8

Learning Objectives

- Identify logical equivalence involving quantifiers and apply De Morgan's laws.
- Apply predicate logic to programming.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.26–28 and pp.62–74.
- Exercises

  p.32 exercises 1–5

  pp.74–75 exercises 1–5 and 8–12.

4.201 De Morgan's laws for quantifiers

The intuition of De Morgan's Laws

Negating quantified expressions is a common activity. Starting with an example.

Let S be the statement *All the university's computers are connected to the network*, and P be the statement *There is at least one computer in the university operating on Linux.*

Intuitively we can find contradictions to both S and P. In the case of S, if we find **at least one** computer **not** connected to the network, then we contradict S. In the case of P, if **not a single** computer operates on Linux, we contradict P. Note that the statement *Not a single computer operates on Linux* is equivalent to *All computers are **not** operating on Linux.*

De Morgan's Laws formalise these intuitions.

De Morgan's Laws

Quantified Expression	Negated Expression
$\forall x P(x)$	$\exists x \neg P(x)$
$\exists x P(x)$	$\forall x \neg P(x)$

Example 1

Let S be the statement *Every student of Computer Science has taken a course in Neural Networks.* Therefore S can be expressed symbolically as $\forall x P(x)$ where $U = \{\text{students in CS}\}$ and $P(x) = x$ has taken a course in Neural Networks.

The negation of S is $\neg S$ which translates to *It is **not** the case that every student in Computer Science has taken a course in Neural Networks.* This statement implies that *There is at least one student of Computer Science who has **not** taken a course in Neural Networks.* Which can be expressed symbolically as $\exists x \neg P(x)$.

Negating nested quantifiers

When we have expressions with nested quantifiers, we simply apply De Morgan's successively from left to right.

$$\begin{aligned} \forall x \exists y \forall z P(x, y, z) &\equiv \exists x \neg \exists y \forall z P(x, y, z) \\ &\equiv \exists x \forall y \neg \forall z P(x, y, z) \\ &\equiv \exists x \forall y \exists z \neg P(x, y, z) \end{aligned}$$

4.203 Rules of inference

Valid argument

In propositional logic, an *argument* is defined as a sequence of propositions. The final proposition is called the *conclusion* and each of the other propositions are called the *premises* (or *hypotheses*).

And *argument* is **valid** if the truth of **all** its premises implies the truth of the *conclusion.*

1. Example 1

   Given the following *argument*:

   - If you have access to the internet, you can order a book in Machine Learning.
   - You have access to the internet

   - $\therefore$ Therefore, you can order a book on Machine Learning.

   This argument is **valid** because whenever all its premises are true, the conclusion must also be true.

2. Example 2

   Given the following *argument*:

- If you have access to the internet, you can order a book in Machine Learning.
- You can order a book on Machine Learning.

- $\therefore$ Therefore, you have access to the internet.

This argument is **not valid** because we can imagine situations where both premises are true, but the conclusion is false.

Rules of inference

These can be seen as **building blocks** for constructing complex valid arguments incrementally.

Given an argument, we could use a truth table to decide whether an argument is true or false, however we will need 2^n rows in the truth table for n variables. This process can be really labor-intensive.

Rules of inference, however, provide a much simpler way of proving the validity of an argument.

Moreover, every rule of inference can be proved using a Tautology[1].

Modus Ponens

Here's the tautology used as the basis for *Modus Ponens*.

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

And the rules of inference

$$\begin{array}{l} p \to q \\ \underline{p \qquad\quad} \\ \therefore q \end{array}$$

And an example

```
p: It is snowing
q: I will study Discrete Mathematics

If it is snowing, I will study Discrete Mathematics.
It is snowing.

Therefore, I will study Discrete Mathematics.
```

Modus Tollens

Tautology shown below is the basis for *Modus Tollens*.

$$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$$

And the rule of inference

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

And an example

```
p: It is snowing
q: I will study Discrete Mathematics

I will not study Discrete Mathematics
If it is snowing, I will study Discrete Mathematics.

Therefore, it is not snowing.
```

Conjunction

The following tautology is the basis for *Conjunction*.

$$((p) \wedge (q)) \rightarrow (p \wedge q)$$

This leads to the following rule of inference

$$\begin{array}{l} p \\ \underline{q} \\ \therefore p \wedge q \end{array}$$

And an example

```
p: I will study Programming
q: I will study Discrete Mathematics

I will study Programming
I will study Discrete Mathematics

Therefore, I will study Programming and Discrete Mathematics
```

Simplification

The next tautology is the basis for *Simplification*

$$(p \wedge q) \rightarrow p$$

It leads to the following valid argument form

$$\frac{p \wedge q}{\therefore p}$$

And an example

```
p: I will study Programming
q: I will study Discrete Mathematics

I will study Programming and Discrete Mathematics

Therefore, I will study Programming
```

Addition

The tautology shown below is the basis for *Addition*

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

It leads to the following valid argument form

$$\frac{p}{\therefore p \vee q}$$

And an example

```
p: I will study Programming
q: I will study Discrete Mathematics

I will study Programming

Therefore, I will study Programming or Discrete Mathematics
```

Hypothetical Syllogism

The tautology that follows is the basis for *Hypothetical Syllogism*

$$(p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$$

It leads to the following valid argument form

$$\frac{\begin{array}{c} p \rightarrow q \\ q \rightarrow r \end{array}}{\therefore p \rightarrow r}$$

And an example

```
p: It is snowing
```

```
q: I will study Discrete Mathematics
r: I will get good grades

If it is snowing, then I will study Discrete Mathematics
If I study Discrete Mathematics, then I will get good grades

Therefore, if it is snowing, then I will get good grades
```

Disjunctive Syllogism

The following tautology is the basis for *Disjunctive Syllogism*

$$((p \vee q) \wedge \neg p) \rightarrow q$$

It leads to the following valid argument form

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

And an example

```
p: I will study Programming
q: I will study Discrete Mathematics

Either I will study Programming or Discrete Mathematics
I will not study Programming

Therefore, I will study Discrete Mathematics
```

Resolution

The next tautology is the basis for *Resolution*

$$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$

It leads to the following valid argument form

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

And an example

```
p: It is raining
q: It is cold
r: It is snowing
```

```
Either it's raining or it's cold
It's not raining or it's snowing

Therefore, It's cold or it's snowing
```

Building valid arguments

1. If it's initially written in English, transform into argument form by assigning variables to each proposition
2. Start with the hypothesis of the argument
3. Build a sequence of steps in which each step follows from the previous by applying **rules of inference** or **laws of logic**
4. The final step is the conclusion

1. Example 1

   Let's build a valid argument from the following premises:

   - *It is not cold tonight*
   - *We will go to the theatre only if it is cold*
   - *If we do not go to the theatre, we will watch a movie at home*
   - *If we watch a movie at home, we will need to make popcorn*

   First, we define our propositional variables:

   - **p**: It is cold tonight
   - **q**: We will go to the theatre
   - **r**: We will watch a movie at home
   - **s**: We will need to make popcorn

   Next, we convert English into logical statements using our propositional variables. We have, respectively:

   - $\neg p$
   - $q \rightarrow p$
   - $\neg q \rightarrow r$
   - $r \rightarrow s$

   Now we can build a valid argument:

	Step	Justification
1	$q \to p$	Hypothesis
2	$\neg p$	Hypothesis
3	$\therefore \neg q$	Modus Tollens 1,2
4	$\neg q \to r$	Hypothesis
5	$\therefore r$	Modus Ponens 3,4
6	$r \to s$	Hypothesis
7	$\therefore s$	Modus Ponens 5,6

Conclusion: We will need to make popcorn

Fallacies

A fallacy is the use of incorrect argument when reasoning. Formal fallacies can be expressed in propositional logic and proved to be incorrect.

Common formal fallacies:

- affirming the consequent
- a conclusion that denies the premises
- contradictory premises
- denying the antecedent
- existential fallacy
- esclusive premises

4.205 Rules of inference with quantifiers

The rules are:

- Universal Instantiation
- Universal Generalisation
- Existential Instantiation
- Existential Generalisation
- Universal Modus Ponens
- Universal Modus Tollens

These rules will either **reintroduce** or **remove** quantifiers within a statement.

Universal Instantiation (UI)

The rule of inference:

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Example:

All Computer Science students study Discrete Mathematics.

$\therefore$ Therefore John, who is a Computer Science student, studies Discrete Mathematics.

Universal Generalisation (UG)

The following rule of inference is used to conclude that a proposition is valid for all members of the Universe of Discourse by showing that it is valid for an arbitrary element in the Universe of Discourse.

$$\frac{P(c)}{\therefore \forall x P(x)}$$

Example:

Let $DS = \{\text{all data science students}\}$ and let c be an arbitrary element in DS.

c studies machine learning.

$\therefore$ Therefore, $\forall x \in DS$, x studies machine learning.

Existential Instatiation (EI)

This is used to conclude that there is an element c for which $P(c)$ is true.

$$\frac{\exists x P(x)}{\therefore P(c)}$$

Example:

Let $DS = \{\text{all data science students}\}$. There exists a student x of data science who uses Python Pandas Library.

$\therefore$ Therefore, there is a student, c, who is using Python Pandas Library.

Existential Generalization (EG)

The existential generalization is used to conclude that $\exists x P(x)$ when $P(c)$ is true for some c.

$$\frac{P(c)}{\therefore \exists x P(x)}$$

Example:

Let $DS = \{\text{all data science students}\}$. John, a student of data science, got an A in the machine learning course.

$\therefore$ Therefore, there exists someone in DS who got an A in machine learning.

Universal Modus Ponens

The Universal Modus Ponens can be thought of as a combination of Universal Instantiation and Modus Ponens.

$$\frac{\begin{array}{l}\forall x P(x) \rightarrow Q(x) \\ P(a)\end{array}}{\therefore Q(a)}$$

Example:

Let $DS = \{\text{all data science students}\}$. Every computer science student studying data science, will study machine learning.

John is studying data science.

$\therefore$ John will study machine learning.

Universal Modus Tollens

Similarly, this can be seen as a combination of Universal Instantiation and Modus Tollens.

$$\frac{\begin{array}{l}\forall x P(x) \rightarrow Q(x) \\ \neg Q(a)\end{array}}{\therefore \neg P(a)}$$

Example:

Let $DS = \{\text{all data science students}\}$. Every computer science student studying data science, will study machine learning.

John is not studying machine learning.

$\therefore$ John is not studying data science.

Expressing complex statements

Given a statement in natural language, we can formalise it by following these steps:

1. Determine the universe of discourse of the variables
2. Reformulate the statement by making **for all** and **there exists** explicit
3. Reformulate the statement by introducing **variables** and defining **predicates**.
4. Reformulate the statement by introducing **quantifiers** and **logical operations**.

1. Example 1

   Express the following statement S: *There exists a real number between any two not equal real numbers.*

   a) The universe of discourse is the set of all real numbers $\mathbb{R}$.

   b) For all real numbers, there exists a real number between any other two real numbers.

   c) For all real numbers x and y, there exists a real number z between x and y.

   d) $\forall x, y \in \mathbb{R}\, \exists z \in \mathbb{R}\, x < z < y$

2. Example 2

   Express the following statement S: *Every student has taken a course in machine learning.*

   a) The universe of discourse is the set of all students CS. Let $M(x)$ be the proposition *has taken a course in machine learning.*

   b) For all students, every student has taken a course in machine learning.

   c) For all students x, x has taken a course in machine learning.

   d) $\forall x\, M(x)$.

   If the Universe of discourse changes, the expression changes:

   a) The universe of discourse is the set of all people. Let $S(x)$ be the proposition *is a student* and $M(x)$ be the proposition *has taken a course in machine learning.*

   b) S can be expressed as $\forall x(S(x) \to M(x))$.

Week 9

Learning Objectives

- Write Boolean expressions.
- Use the laws of Boolean algebra to simplify Boolean expressions.
- Represent a Boolean function.
- Simplify logic circuits/expressions.
- Convert truth tables into Boolean expressions and vice versa.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.811–821.
- Exercises

  pp.818–819 exercises 1–5, 20–25 and 35–40.

For gates and circuits, see the Essential reading for Week 2.

5.101 Introduction to Boolean algebra

History of Boolean Algebra

Between 384-322C Aristotle established the foundation of Logic in his *Organon*. Later in 1854, George Boole, an English Mathematician and Logician, published An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities, which developed a system of *Logical Algebra* by which reasoning can be expressed mathematically.

In 1904, Edward V. Huntington, an American Mathematician, published Sets Of Independent Postulates For The Algebra Of Logic in which he defined 6 rules (or postulates) of Boolean Algebra.

In 1938, Claude Shannon published his Master's Thesis entitled A Symbolic Analysis of Relay and Switching Circuits. In this thesis, Shannon proved that Boolean Algebra could be used to simplify the arrangement of relays; essentially demonstrating that Boolean Algebra could be used to simplify logic.

Applications of Boolean Algebra

Boolean Algebra is the basic building block of computer circuit analysis.

System requirements can be converted into Boolean Algebra and implemented as a circuit. For example, if we have the requirement:

- *When the system is activated, a fire sprinkler should spray water if high heat is detected* could be implemented as follows:

  $$w = hANDa$$

  where h represents *high heat detected*, a represents *system activated* and w represents *spraying water*.

Two-valued Boolean Algebra

The most well-known and widely used for of Boolean Algebra. Variables are binary, therefore they can only accept values of the set $\{0, 1\}$. The operators $+$ and $\cdot$ correspond to OR and AND respectively.

This form of Boolean Algebra can be used to specify and design digital circuits.

Operations of Boolean Algebra

There are three fundamental operations in Boolean Algebra.

- **AND**

  Also referred to as *logical product*, *intersection* or *conjunction*. Can be represented as $x \cdot y$, $x \cap y$ or $x \wedge y$.

  Truth Table is as follows:

x	y	$x \cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

- **OR**

  Also referred to as *logical sum*, *union* or *disjunction*. Can be represented as $x + y$, $x \cup y$ or $x \vee y$.

  Truth Table is as follows:

x	y	x_y
0	0	0
0	1	1
1	0	1
1	1	1

- **NOT**

  Also referred to as *logical complement* or *negation*. Can be represented as x', $\bar{x}$ or $\neg x$.

  Truth Table is as follows:

x	$\bar{x}$
0	1
1	0

When parentheses are not used, these three operators have the following order of precedence: **NOT** > **AND** > **OR**. Note that this still respects the same order of precedence defined in Precedence of logical operators.

5.103 Postulates of Boolean algebra

Huntington's postulates

There 6 axioms defined by Huntington's postulates. These 6 axioms must be satisfied by any Boolean Algebra.

The axioms are:

- **Closure**

  any result from logical operation must belong to the set $\{0, 1\}$.

- **Identity**

  The logical sum identity $x + 0 = x$ and the logical product identity $x \cdot 1 = x$.

- **Commutativity**

  Both logical sum and logical product are commutative, therefore $x + y = y + x$ and $x \cdot y = y \cdot x$.

- **Distributivity**

  Both logical sum and logical product and distributive between each other, therefore $x \cdot (y + z) = x \cdot y + x \cdot z$ and $x + (y \cdot z) = (x + y) \cdot (x + z)$.

- **Complement**

  Complements exist for all elements: $x + \bar{x} = 1$ and $x \cdot \bar{x} = 0$.

- **Distinct Elements**

  This states that any Boolean Algebra has to have two distinct values, therefore $0 \neq 1$.

Basic theorems

Using the 6 axioms from previous sections, we can establish other useful theorems for designing and analysing digital circuits.

Logical Sum	Theorem	Logical Product
$x + x = x$	**Idempotent Laws**	$x \cdot x = x$
$x + 1 = 1$	**Tautology and Contradiction**	$x \cdot 0 = 0$
$\bar{\bar{x}} = x$	**Involution**	
$(x + y) + z = x + (y + z)$	**Associative Laws**	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
$x + (x \cdot y) = x$	**Absorption Laws**	$x \cdot (x + y) = z$
if $y + x = 1$ and $y \cdot x = 0$, then $x = \bar{y}$	**Uniqueness of Complement**	
$\bar{0} = 1$ and $\bar{1} = 0$	**Inversion Law**	

De Morgan's Theorems

Theorem 1 (De Morgan's Theorem 1)**.** *The complement of a logical product or variables is equal to the logical sum of the complements of the variables.* $\overline{x \cdot y} = \bar{x} + \bar{y}$.

Theorem 2 (De Morgan's Theorem 2)**.** *The complement of a logical sum or variables is equal to the logical product of the complements of the variables.* $\overline{x + y} = \bar{x} \cdot \bar{y}$.

Principle of duality

Starting with a Boolean Relation, we can build another equivalent Boolean Relation by:

- Changing every $+$ to $\cdot$
- Changing every $\cdot$ to $+$
- Changing every 0 to 1
- Changing every 1 to 0

For example $A + B \cdot C \equiv A \cdot (B + C)$.

Ways of proving theorems

There are 4 ways to prove the equivalence of Boolean relations

- **Perfect Induction**

  Show that both relations have identical truth tables. This can be tedious as the number of variables grow.

- **Axiomatic Proof**

  Apply Huntington's postulates or theorems to the expressions until identical expressions are found.

- **Duality Principle**

  Every theorem remain valid after application of the Duality Principle.

- **Contradiction**

  Assuming the hypothesis is false and then proving that the conclusion is also false.

1. Example: Absorption Rule

   This rule can be proved easily with a truth table:

x	y	$x + (x \cdot y)$
0	0	0
0	1	0
1	0	1
1	1	1

   It can also be proved directly:

$$\begin{aligned} x + (x \cdot y) &\equiv (x \cdot 1) + (x \cdot y) \\ &\equiv x \cdot (1 + y) \\ &\equiv x \cdot 1 \\ &\equiv x \end{aligned}$$

   To prove the second part of the absorption law, we can use the duality principle, therefore $x + (x \cdot y) = x = x \cdot (x + y)$.

5.105 Boolean functions

Definition

Definition 22 (Boolean Function)**.** *A Boolean Function defines a mapping from one or multiple Boolean input values to a Boolean output value.*

For n input values, there are 2^n possible combinations.

Given a function f with 3 input values, f can be completely defined with a table of 8 rows:

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

Algebraic forms

There is a single way of representing a Boolean function in a truth table, however algebraically a function can be represented in a variety of forms. For example $f(x) = x + \bar{x} \cdot y = x + y$.

Standardised forms of a function

Boolean functions are standardised to be represented either a *sum-of-products* or *product-of-sums*.

The *sum-of-products* is a function of the form $f(x,y,z) = xy + xz + yz$, while a *product-of-sums* is a function of the form $f(x,y,z) = (x+y) \cdot (x+z) \cdot (y+z)$.

The *sum-of-products* form is, usually, easier to use and simplify.

Build a *sum-of-products* form

Building *sum-of-products* from a truth table is simple.

1. Look at values of the variables that make the function evaluate to 1.
2. If an input is 1, it appears *uncomplemented* in the expression
3. If an input is 0, it appears *complemented* in the expression
4. The function f is, then, represented as a *sum-of-products* of all the terms for which the function is 1.

1. Example

   Given the truth table below, represent the function as a *sum-of-products*.

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

Therefore, $f(x, y) = \bar{x}y + x\bar{y} + xy$.

Useful functions

The *exclusive-or* function $x \oplus y$ is true when either x or y is true, but not both. This can be expressed as $f(x, y) = \bar{x}y + x\bar{y}$.

The *implies* function $x \to y$ is false when x is true and y is false, and true otherwise. This can be expressed $f(x, y) = \bar{x} + y$.

Week 10

Learning Objectives

- Write Boolean expressions.
- Use the laws of Boolean algebra to simplify Boolean expressions.
- Represent a Boolean function.
- Simplify logic circuits/expressions.
- Convert truth tables into Boolean expressions and vice versa.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.15–21.
- Exercises

  p.22 exercises 23 and 24.

5.201 Logic gates

Definition of a gate

A Logic Gate is the basic element of circuits implementing a Boolean operation. The most elementary of such gates are the **OR** gate, the **AND** gate and the **NOT** (or inverter) gate.

All Boolean functions can be written in terms of these three logic gates.

AND Gate

The AND Gate produces a *HIGH* output (value 1) when all its inputs are *HIGH*; otherwise, the output *LOW* (value 0).

The AND Gate is represented as show in figure 0.1, below we show its truth table:

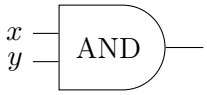


Figure 0.1: A 2-input AND Gate

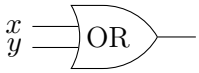


Figure 0.2: A 2-input OR Gate

x	y	$x \cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

Note that $f = x \cdot y$ can also be written as $f = xy$.

OR Gate

The OR Gate produces a *HIGH* output (value 1) when at least one of its inputs are *HIGH*; otherwise, the output *LOW* (value 0).

The OR Gate is represented as show in figure 0.2, below we show its truth table:

x	y	$x + y$
0	0	0
0	1	1
1	0	1
1	1	1

Inverter Gate

The Inverter Gate produces a *HIGH* output (value 1) when its input is *LOW*; and produces a *LOW* when its input is *HIGH*.

The Inverter Gate is represented as show in figure 0.3, below we show its truth table:

x	$\bar{x}$
0	1
1	0

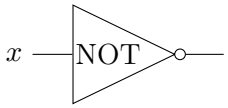


Figure 0.3: An Inverter Gate

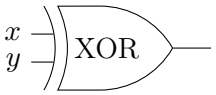


Figure 0.4: A 2-input XOR Gate

XOR Gate

The XOR Gate produces a *HIGH* output (value 1) its inputs have different values and a *LOW* otherwise.

The XOR Gate is represented as show in figure 0.4, below we show its truth table:

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

NAND Gate

Equivalent to "not AND", so this is the inversion of the AND Gate. The NAND Gate is represented as show in figure 0.5.

NOR Gate

Similarly, this is the inversion of the OR Gate. The NOR Gate is represented as show in figure 0.6.

XNOR Gate

The inversion of the XOR Gate. The XOR Gate is represented as show in figure 0.7.

Figure 0.5: A 2-input NAND Gate

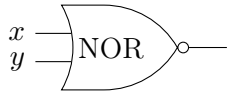


Figure 0.6: A 2-input NOR Gate

Figure 0.7: A 2-input XNOR Gate

Multiple input gates

AND, OR, XOR and XNOR are all **commutative** and **associative** operations. All of them can be extended to more than 2 inputs as shown in figure 0.8.

NAND and NOR are both **commutative** but **not associative**. Extending number of inputs is less obvious. We must use parentheses correctly when cascading NAND and NOR operations.

Representing De Morgan's Laws

- **Theorem 1**

  $\overline{x \cdot y} \equiv \bar{x} + \bar{y}$.

  This says that figure 0.9 is equivalent to 0.10.

- * Theorem 2*

  This says that figure 0.11 is equivalent to 0.12.

5.203 Combinational circuits

Definition of circuit

A *Combinational Circuit* is a combination of different logic gates designed to model a Boolean function. In other words, a Combinational Circuit **implements** a particular Boolean function.

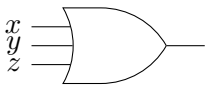


Figure 0.8: A 3-input OR Gate

Figure 0.9: A 2-input NAND Gate

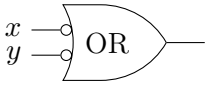


Figure 0.10: A 2-input OR Gate with negated inputs

Building a circuit from a function

Given a particular boolean function, we can implement a logic circuit representing **all** states of the function.

Intuitively, we want to **minimise** the number of logic gates used in order to minimize the **cost** of producing the circuit.

For example, let's build a circuit for the function f defined as $f(x, y, z) = x + \bar{y}z$. See figure 0.13 for the result.

Writing Boolean expressions from a circuit

Given a logic network, we can write its Boolean expression as follows:

1. **Label** all gate outputs that are a function of input variables
2. **Express** the Boolean functions for each gate in the first level
3. **Repeat** until all outputs of the circuit are written as Boolean expressions

1. Example

   Consider the circuit in 0.14. Figures 0.15, 0.16, and 0.17 show the steps necessary to extract a Boolean expression from a circuit layout.

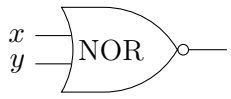


Figure 0.11: A 2-input NOR Gate

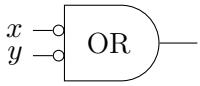


Figure 0.12: A 2-input AND Gate with negated inputs

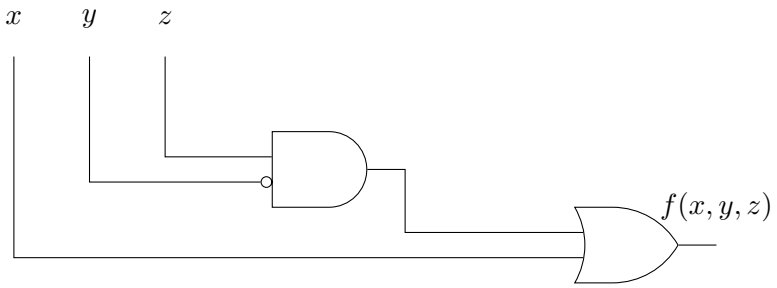


Figure 0.13: $f(x, y, z) = x + \bar{y}z$

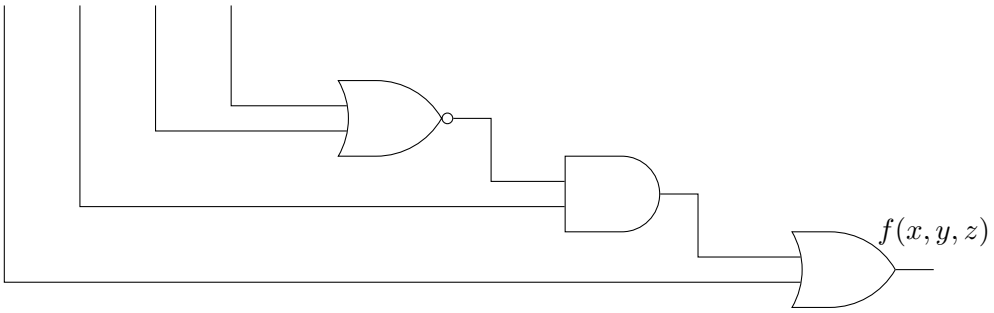


Figure 0.14: Logic Circuit to extract Boolean expression

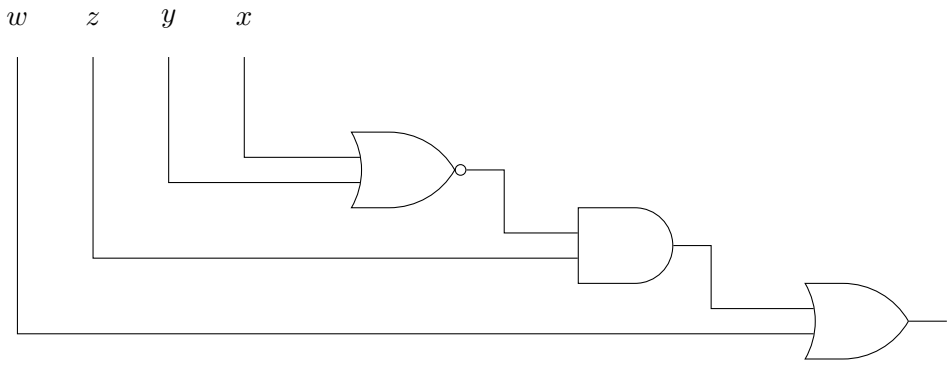


Figure 0.15: Logic Circuit: Label Inputs

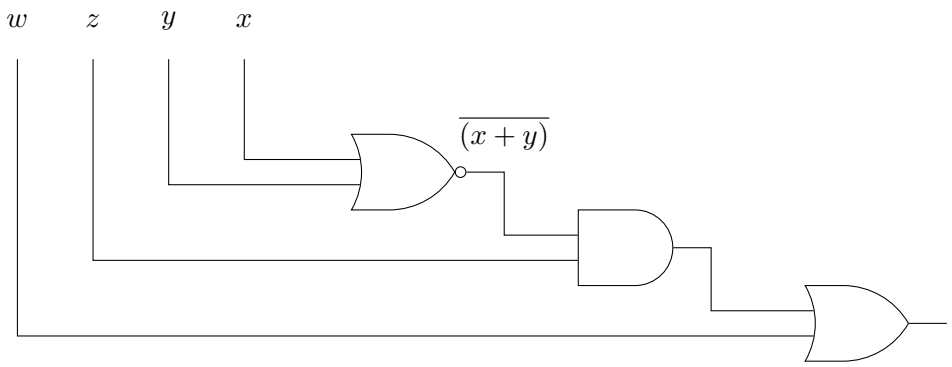


Figure 0.16: Logic Circuit: Express Boolean Expression of first level

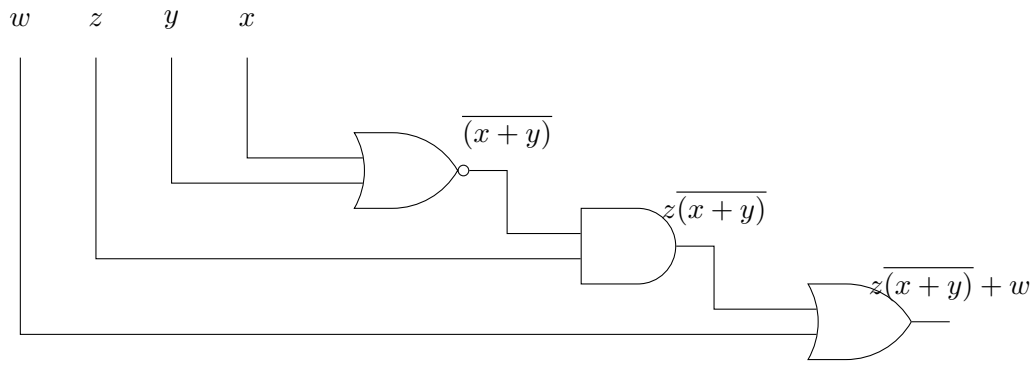


Figure 0.17: Logic Circuit: Repeat for other levels

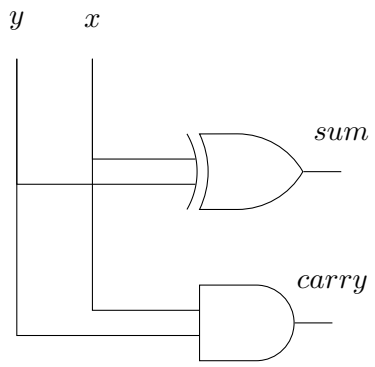


Figure 0.18: 1-bit half-adder

Building a circuit to model a problem

Combinational circuits are useful for designing systems that solve a specific problem. When we want to build a combinational circuit to solve a problem we follow these steps:

1. **Label** inputs and outputs using variables
2. **Model** the problem as Boolean expression
3. **Replace** each operation by equivalent logic gate

Building an adder circuit

We're going to build a Half-adder circuit for two 1-bit inputs and a carry out signal.

The truth table is as follows:

x	y	sum	$carry$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

If we look closely, the colum *sum* contains the the truth table for an exclusive or gate while the colum *carry* contains the truth table for an and gate. Therefore, our circuit is shown in figure 0.18.

Note that a half-adder is not useful for multi-bit additions since it lacks a carry input signal.

Building a full adder

To overcome the limitations of a half-adder, we can transform it into a full adder by adding a carry input and including gates for processing the carry input.

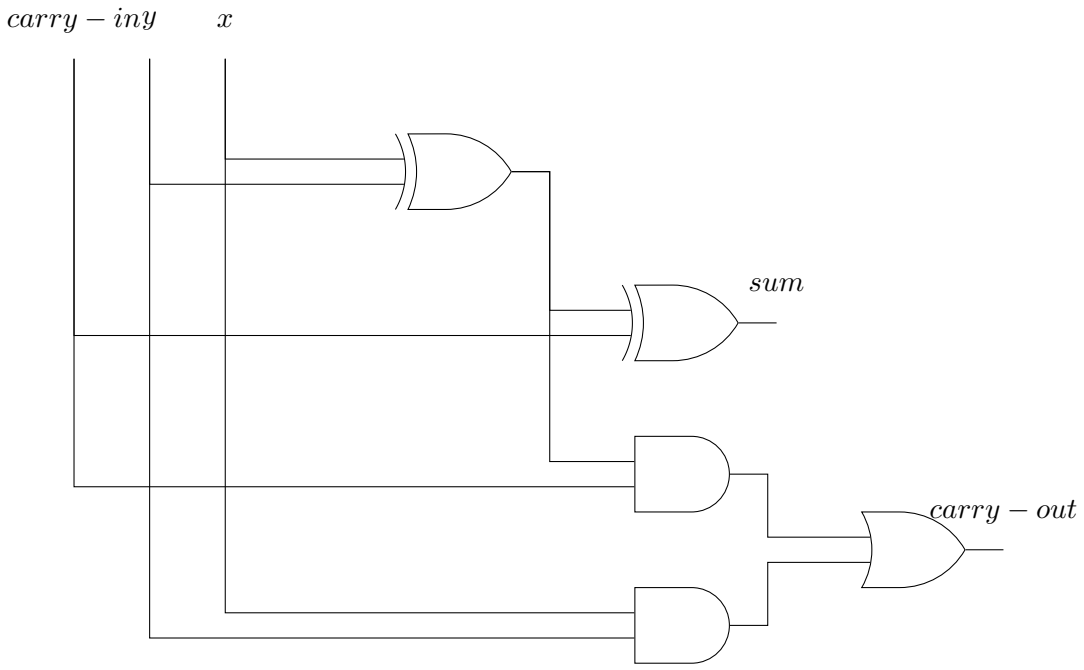


Figure 0.19: 1-bit full-adder

The new truth table is as follows:

x	y	$carry-in$	sum	$carry-out$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

We can see here that $sum = x \oplus y \oplus carry-in$ and $carry-out = xy + carry-in \cdot (x \oplus y)$.

The corresponding circuit is shown in figure 0.19.

5.205 Simplification of circuits

Benefits of Simplification

Every function can be written as a sum-of-products, however this may not be the optimal solution in terms of number of gates and the depth of the circuit.

This is why circuits need to be simplified.

Simplification – also referred to as minimisation or optimisation – is benefitial in circuit design for the following reasons:

- Reduces the cost of circuits by reducing the number of gates used
- May reduce the computation time
- Allows more logic to fit into the same area

Algebraic simplification

A technique based on the application of Boolean algebra theorems to simplify the behavior of Boolean functions.

To produce a sum-of-product expression, we usually need to rely on at least one of the following theorems:

- De Morgan's laws and involution
- Distributive laws
- Commutative laws
- Idempotent laws
- Complement laws
- Absorption laws

1. Example

   Simplify the following Boolean expression:

$$E = \overline{\overline{(\overline{(xy)}z)}}\,\overline{((\bar{x}+z)(\bar{y}+\bar{z}))}$$

$$\begin{aligned}
&\equiv (\overline{\overline{(xy)}} + \bar{z})\overline{((\bar{x}+z)(\bar{y}+\bar{z}))} \\
&\equiv (xy + \bar{z})(\overline{(\bar{x}+z)} + \overline{(\bar{y}+\bar{z})}) \\
&\equiv (xy + \bar{z})(\bar{\bar{x}}\bar{z} + \bar{\bar{y}}\bar{\bar{z}}) \\
&\equiv (xy + \bar{z})(x\bar{z} + yz) \\
&\equiv xyx\bar{z} + xyyz + \bar{z}x\bar{z} + \bar{z}yz \\
&\equiv xy\bar{z} + xyz + x\bar{z} \\
&\equiv xy + x\bar{z}
\end{aligned}$$

Karnaugh maps

A Karnaugh Map (or K-map) is a graphical representation of Boolean functions and is different from a truth table. Adjacent cells in a K-map only change one variable.

	$\bar{y}$	y
$\bar{x}$	0	0
x	1	1

1. Example

   Consider the Boolean function represented by the truth table below:

x	y	z	f
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	1

   Since we have three variables, we need a K-map of three inputs:

	$\bar{y}\bar{z}$	$\bar{y}z$	yz	$y\bar{z}$
$\bar{x}$	0	0	1	0
x	1	1	1	1

   In this case, the expression is $x + yz$.

Week 11

Learning Objectives

- State the principle of mathematical induction.
- Discuss the ideas of the base step and inductive step in a proof by mathematical induction.
- Apply the ideas of mathematical induction to recursion and recursively defined structures.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.307–325 and pp.328–336.
- Exercises

  pp.325–326 exercises 1, 2, 6, 7, 15 and 16

  p.338 exercises 19–21.

For recursion, see the Essential reading for Week 2

6.101 Introduction to proofs

We start with some definitions and terminology and how to formalize a theorem. Then we continue with three types of proofs: direct proof, proof by contraposition, and proof by contradiction.

A proof is, simply put, a valid argument used to prove the truth of a mathematical statement. In order to build a proof, we must rely on all the knowledge introduced previously:

- Variables
- Predicates
- Quantifiers
- Laws of Logic
- Rules of inference

Terminology

Theorem A formal statement that can be shown to be true

Axiom A statement assumed to be true to serve as a premise to further arguments

Lemma A proven statement used as a step to a larger result rather than as a statement of interest by itself

Corollary A theorem that can be established by a short proof from a theorem

Formalising a theorem

The statement **S** *There exists a real number between any two non-equal real numbers* can be formalized as:

Theorem 3. $\forall x, y \in \mathbb{R} x < y \rightarrow \exists z \in \mathbb{R} \mid x < z < y$

Direct proof

A Direct Proof is simply a demonstration that a conditional statement $p \rightarrow q$ is true.

We always with the assumption that p is true, then we employ **axioms**, **definitions**, and **theorems**, together with **rules of inference**, to show that q must also be true.

For example, let's prove our theorem defined in section Formalising a theorem.

Proof. Let x and y be arbitrary elements in $\mathbb{R}$. Let's assume $x < y$.

Let $z = \frac{x+y}{2}$. $z \in \mathbb{R}$, satisfying $x < z < y$.

Using the Universal Generalization rule of inference, we can conclude:

$\therefore \forall x, y \in \mathbb{R} x < y \rightarrow \exists z \in \mathbb{R} \mid x < z < y$ □

Proof by contrapositive

A Proof by Contrapositive is a proof technique that relies on the fact that proving $p \rightarrow q$ is equivalent to proving $\neg q \rightarrow \neg p$.

We start the proof by assuming $\neg q$ is true, then use **axioms**, **definitions**, and **theorems**, together with **rules of inference**, to show that $\neg p$ must also be true.

For example, let's prove the theorem *If n^2 is even, then n is even.*

Proof. Let's assume n is odd. Then $\exists k \in \mathbb{Z} \mid n = 2k+1$. Then $\exists k \in \mathbb{Z} \mid n^2 = (2k+1)^2 = 2(2k^2 + 2k) + 1$. Then, n^2 is also odd. Therefore, we conclude that if n is odd, then n^2 is also odd. □

Proof by contradiction

A Proof by Contradiction is a form of proof which relies on assuming the premise to be false and showing that it leads to a contradiction.

We start the proof by assuming $\neg p$ to be true\ then use **axioms**, **definitions**, and **theorems**, together with **rules of inference**, to show that $\neg p$ is false. We can conclude, therefore, that assuming $\neg p$ was wrong, so it must be true.

For example, let's prove the theorem *There are infinitely many prime numbers.*

Proof. Let's suppose there are finitely many prime numbers and list them as $p_1, p_2, p_3, \ldots, p_n$.

Let's consider the number $c = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$, the product of all primes + 1.

As c is a natural number, it has at least one prime divisor. Then, $\exists k \in \{1, \ldots, n\} \mid p_k / c$. Then, $\exists k \in \{1, \ldots, n\} \exists d \in \mathbb{N} \mid d \cdot p_k = c = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$.

Then, $\exists k \in \{1, \ldots, n\} \exists d \in \mathbb{N} \mid d = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_{k-1} + p_{k+1} + \ldots + p_n + \frac{1}{p_k}$. □

6.103 The principle of mathematical induction

Mathematical Induction can be used to assert that a propositional function $P(n)$ is true for all positive integers n. In other words, given a propositional function $P(n)$, we can use mathematical induction to show that $P(n)$ holds for all n.

It can formalised using the following rule of inference:

$$\frac{\begin{array}{l} P(1) \text{is true} \\ \forall k(P(k) \to P(k+1)) \end{array}}{\therefore \forall n P(n)}$$

The intuition behind induction

Let $P(n)$ be the propositional function verifying:

- $P(1)$ is true
- $\forall k(P(k) \to P(k+1))$

Intuitively, we can say that P is true for 1. Since P is true for 1, then it is true for 2. Since it is true for 2, then it is true for 3, and so on. Since P is true for $n-1$, it's true for n.

What this means is that the **Base Case** $P(1)$ shows that the property holds true initially. The **Inductive Step** $\forall k(P(k) \to P(k+1))$ shows tha the property holds for all k by showing how each iteration influences the next.

Structure of induction

In order to complete a proof by induction for a propositional function $P(n)$, we need to verify two steps:

Base Case Prove that $P(1)$ is true

Inductive Step Prove that $\forall k \in \mathbb{N} P(k) \rightarrow P(k+1)$[1]

Some uses of induction

Mathematical induction can be used to proce that $P(n)$ is true for all integers greater than a particular threshold, where $P(n)$ is a propositional function. This might cover multiple cases:

- Proving formulas
- Proving inequalities
- Proving divisibility
- Proving properties of subsets and their cardinality

6.106 Proof by induction

Mathematical Induction is a proof technique which allows us to prove that a property holds for all natural numbers.

Proving formulas

Let's prove $P(n) : 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

Proof. We start with the base case:

$$\begin{aligned} 1 &= \frac{1(1+1)}{2} \\ 1 &= \frac{1(2)}{2} \\ 1 &= \frac{2}{2} \\ 1 &= 1 \end{aligned}$$

Then we move on to the inductive step:

[1] $P(k)$ is referred to as the **inductive hypothesis**

$$
\begin{aligned}
1+2+3+\ldots+k &= \frac{k(k+1)}{2} \\
1+2+3+\ldots+k+(k+1) &= \frac{(k+1)(k+2)}{2} \\
\frac{k(k+1)}{2}+(k+1) &= \frac{(k+1)(k+2)}{2} \\
\frac{k(k+1)+2(k+1)}{2} &= \frac{(k+1)(k+2)}{2} \\
\frac{(k+1)(k+2)}{2} &= \frac{(k+1)(k+2)}{2}
\end{aligned}
$$

We have shown that the property holds for the base case and for the inductive step, therefore the proof is complete. □

Proving inequalities

Let's prove $P(n) : 3^n < n!$ if $n \geq 7$.

Proof. We start with the base case:

$$
\begin{aligned}
3^7 &< 7! \\
2187 &< 5040
\end{aligned}
$$

Then we move on to the inductive step.

$$
\begin{aligned}
3^k &< k! \\
3^{k+1} &< (k+1)! \\
3 \cdot 3^k &< (k+1) \cdot k!
\end{aligned}
$$

We have shown that the property holds for the base case and for the inductive step, therefore the proof is complete. □

Proving divisility

Let's prove $P(n) : \forall n \in \mathbb{N} 5 | 6^n + 4$.

Proof. We start with the base case:

$$
\begin{aligned}
5 | 6^0 + 4 \\
5 | 1 + 4 \\
5 | 5
\end{aligned}
$$

Then we move on to the inductive step.

$$5|6^k + 4$$

Let $6^k + 4 = 5p$, then $5p - 4 = 6k$.

$$\begin{aligned}
&5|6^{k+1} + 4\\
&5|6 \cdot 6^k + 4\\
&5|6(5p - 4) + 4\\
&5|30p - 24 + 4\\
&5|30p - 20\\
&5|5(6p - 4)
\end{aligned}$$

We have shown that the property holds for the base case and for the inductive step, therefore the proof is complete. □

6.108 Strong induction

Strong Induction is a form of mathematical induction which makes the inductive step easier to prove by using a stronger hypothesis. We assume that the property holds for all k less than k + 1.

In other words, we employ the conditional statemente $P(1), P(2), \ldots, P(k) \rightarrow P(k+1)l$

Strong induction

It can formalised using the following rule of inference:

$$\frac{\begin{array}{l}P(1)\text{is true}\\ \forall k(P(1), P(2), \ldots, P(k) \rightarrow P(k+1))\end{array}}{\therefore \forall n P(n)}$$

It's sometimes called **Complete Induction**.

Example

Let's prove $P(n) : \forall n \in \mathbb{N} \wedge n \geq 2, n$ is divisible by a prime number.

Proof. We start with the base case, which reduces to 2. 2 is a prime number and divides itself.

Then we move on to the inductive step. Let $k \in \mathbb{N}$, greater than 2. If the inductive hypothesis $P(k)$ is true, let's assume $P(2), \ldots, P(k+1)$ is true. Then, $\forall m \in \mathbb{N}$ and $2 \leq m \leq k+1$, $\exists p$ a prime number dividing m.

Here we have two cases:

$k+2$ **is a prime number** then $k+2$ is trivially divisible by itself

$k+2$ **is a composite number** then $\exists m$ dividing $k+2$. Because $2 \leq m \leq k+1$, then $\exists p$ dividing m, which also divides $k+2$.

We have shown that the property holds for the base case and for the inductive step, therefore the proof is complete. □

Well-ordering property

It is an axiom about $\mathbb{N}$ that we assume to be true. The axioms about $\mathbb{N}$ are as follows:

1. The number 1 is a positive integer
2. If $n \in \mathbb{N}$, then $n+1$ is also a positive integer
3. Every positive integer other than 1, is the successor of a positive integer
4. The Well-ordering property: every non-empty subset of the set of positive integers has a least element

The well-ordering property can be used as a tool in building proofs.

Example

Let's reconsider our previous proof.

Proof. Let S be the set of positive integers greater than 1 without a prime divisor.

Suppose S is non-empty. Let n be its smallest element. n cannot be prime since n divides itself if n is prime; i.e. n would be its own prime divisor.

Therefore, n must be composite, which means it must have a divisor d such that $1 < d < n$ Then d must have a prime divisor.

Let p be the prime divisor of d. We know that p/d and d/n, therefore p/n, which contradicts our statement that S is the set of positive integers greater than 1 without a prime divisor.

Therefore, S must be an empty set, which verifies $P(n)$. □

Equivalence of the three concepts

- mathematical induction → well-ordering property
- well-ordering property → strong induction
- strong induction → mathematical induction

All three concepts are equivalent.

Week 12

Learning Objectives

- Describe the concept of recursion and give examples of its application.
- Identify the base case and the general case of a recursively defined problem.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.339–351.
- Exercises

  p.351 exercises 1–9 and 15–17.

6.201 Recursive definitions

Definition

When we define a mathematical object in terms of itself, this is called Recursion.

Recursively defined functions

A recursively defined function f with domain $\mathbb{N}$ is defined by:

Basis Step initial value of the function

Recursive Step a rule for finding the value of the function at an integer from its previous values.

For example the Fibonacci function can be defined as:

$$\begin{cases} f(0) & 1 \\ f(1) & 1 \\ f(n) & f(n-1) + f(n-2) \end{cases}$$

Recursively defined sets

A recursively defined set S, is defined by:

Basis Step initial elements of the set

Recursive Step a rule for generating new elements from the ones we already have

For example, the set S is recursively defined by:

Basis Step $4 \in S$

Recursive Step $x \in S \wedge y \in S \rightarrow x + y \in S$

Recursive algorithms

An algorithm is a finite sequence of precise instructions for performing a computation or for solving a problem.

A recursive algorithm is an algorithm which solves a problem by reducing it to a smaller instance of the same problem with smaller input.

For example, here's a recursive algorithm for computing $n!$:

Algorithm 1 Computing $n!$

```
1: function FACTORIAL(n)
2:     if n = 0 then
3:         return 1
4:     return n× FACTORIAL(n − 1)
```

6.204 Recurrence relations

Definitions

A Recurrence Relation is an equation that defines a sequence based on a rule that produces the next term as a function of the previous.

An infinite sequence is a function from the set of integers to the set of real numbers.

In many cases, it's useful to formalise a problem as a sequence before solving it.

Linear recurrences

A relation in which each term of the sequence is a linear function of earlier terms.

There are two types of linear recurrences:

Linear Homogenous Recurrences $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$. $c_1, \ldots, c_k \in \mathbb{R}$. k is the degree of the relation.

Linear Non-homogenous Recurrences $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} + f(n)$. $c_1, \ldots, c_k \in \mathbb{R}$. k is the degree of the relation.

Arithmetic sequences

A sequence is called arithmetic if the **difference** between consecutive terms is a constant c.

Geometric sequences

A sequence is called geometric if the **ratio** between consecutive terms is a constant r.

Divide and conquer recurrence

A divide and conquer algorithm consists of three steps:

- Dividing the problem into smaller subproblems
- Solving each subproblem recursively
- Combining all solutions to find a final solution to the original problem

6.206 Solving recurrence relations

Solving linear recurrence

Let:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$$

be a linear homogenous recurrence. If a combination of the geometric sequence:

$$a_n = r^n$$

is a solution to this recurrence, it satisfies:

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \ldots + c_k rn - k$$

By dividing both sides by r^{n-k} we get:

$$r^k = c_1 r^{k-1} + c_2 r^{k-2} + \ldots + c_k$$

This equation is called the **characteristic equation**. Solving this equation is the first step towards finding a solution to the linear homogenous recurrence.

If r is a solution of the equation with multiplicity p, then the combination:

$$(\alpha + \beta n + \gamma n^2 + \ldots + \mu n^{p-1})r^n$$

satisfies the recurrece.

Induction for solving recurrence

Sometimes it's easier to solve a recurrence relation using strong induction.

Week 13

Learning Objectives

- Define a graph, edges, vertices, parallel edges, loops, cycles and walk, path and connected graphs.
- Describe the degree sequence of a graph and the relation that links the sum of the degree sequence.
- Describe special graphs: simple graphs, complete graphs and r-regular graphs.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.617–625, pp.627–631, pp.637–640 and pp.666–676.
- Exercises

  pp.625–626 exercises 1–3, 18, 19 and 20

  pp.641–642 exercises 1–10 and 28–32

  pp.676–677 exercises 1–4 and 12–23.

7.101 Introduction

We start studying Graphs. Graphs are discrete structures consisting of vertices and edges connecting them.

Graph Theory is a branch of discrete mathematics which studies these structures.

Applications of Graphs

- Modeling computer networks
- Modeling road maps
- Solving shortest-path problems between cities
- Assigning jobs to employees
- Distinguishing chemical compound structures

- Modeling molecules

7.103 Definition of a graph

Graph

A graph G is an ordered triple $G = \{V, E\}$, where V is the set of vertices and E is the set of edges.

Vertex

The basic element of a graph, drawn as a node or a dot. The set of vertices of G is usually denoted by $V(G)$ or simply V. Figure 0.1 denotes a graph with 3 vertices.

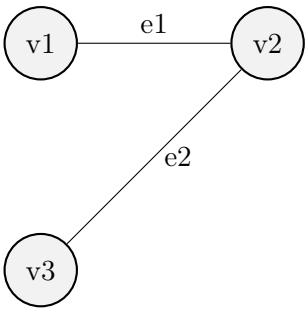


Figure 0.1: A sample graph with 3 vertices

In the graph shown in figure 0.1, $V(G) = \{v1, v2, v3\}$.

Edge

A link between two vertices. It's drawn as line connecting exactly two vertices. The set of edges in a graph G is denoted by $E(G)$ or simply E.

In the graph shown in figure 0.1, $E(G) = \{e1, e2\} = \{\{v1, v2\}, \{v2, v3\}\}$.

Adjacency

- Two vertices are adjacent if they are endpoints on the same edge
- Two edges are adjacent if they share the same vertex
- If vertex v is and endpoint of edge e, then we say that v and e are incident

Loops and parallel edges

Let's consider the following graph:

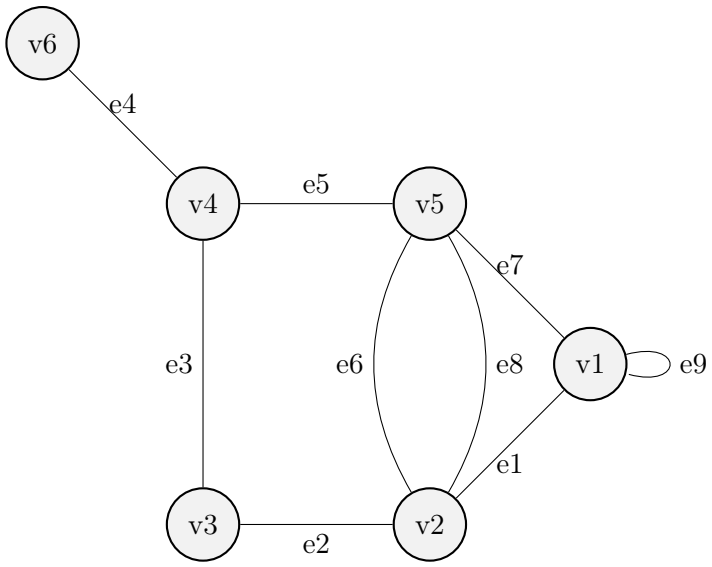


Figure 0.2: Loops and Parallel Edges

The vertices $v2$ and $v5$ are linked with two edges ($e6$ and $e8$), those edges are referred to as **parallel edges**.

The vertex $v1$ is linked to itself by edge $e9$, that edge is called a **loop**.

Directed Graph - Digraph

A direct graph is a graph in which the edges have a direction, indicated with an arrow on the edge. In the graph shown in figure 0.3, we can see that $e1$ is a connection from $v1$ to $v2$ but it is **not** a connection from $v2$ to $v1$.

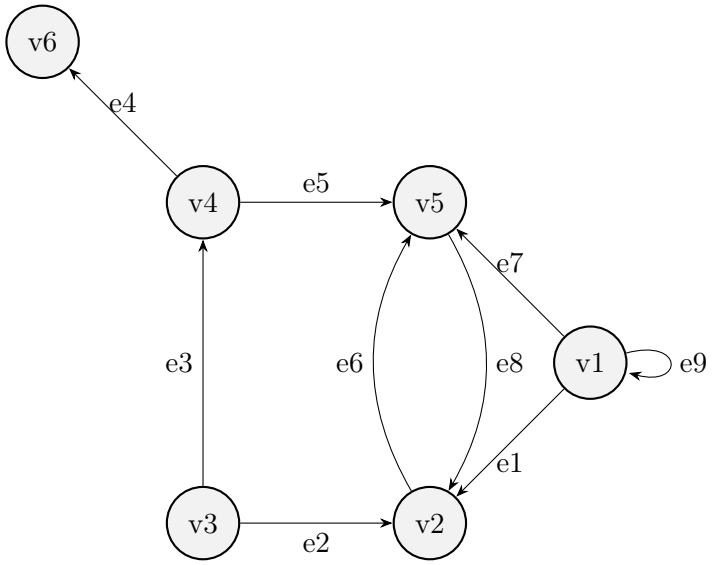


Figure 0.3: A directed graph

7.105 Walks and paths in a graph

Definition of a walk

A walk is a sequence of vertices and edges of a graph where vertices and edges can be repeated.

A walk of length k is a succession of k (not necessarily different) edges of the form:

$$uv, vw, wx, \ldots, yz$$

Taking the graph in figure 0.1 as an example, we can define a walk of length 4 from $v1$ to $v6$:

$$v1v2, v2v3, v3v4, v4v6 = e1, e2, e3, e4 = v1v2v3v4v6$$

Definition of a trail

A trail is a walk in which no edge is ever repeated. Vertices can be repeated, but no edges can be repeated.

Definition of a circuit

A circuit is a closed trail, meaning the starting and ending vertices are the same. Only vertices can be repeated.

Definition of a path

A path is a trail in which neither vertices nor edges are repeated.

Definition of a cycle

A cycle is a closed path in which a vertex is reachable from itself.

Eulerian path

An Eulerian path is a path that uses each edge precisely once. If such a path exists, the graph is called **traversable**.

Hammiltonian path

A Hammiltonian path (or traceable path) is a path that visits each vertex precisely once. If such a path exists, the graph is called a **traceable graph**.

Hammiltonian cycle

A cycle that uses each vertex exactly once (except for the starting vertex, which is visited exactly twice) is called a Hammiltonian cycle. If such a cycle exists, the graph is called a **Hammiltonian graph**.

Connectivity

An **undirected** graph is **connected** if you can get from any node to any other node by following a sequence of edges. This means that any two random nodes in a graph are connected by a path.

The graph depicted in figure 0.4 is a connected graph while the graph depicted in figure 0.5 is **not** a connected graph.

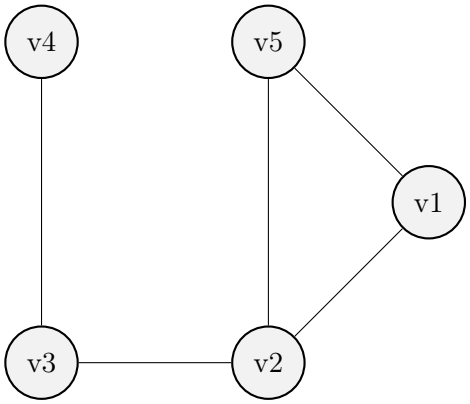


Figure 0.4: A Connected Graph

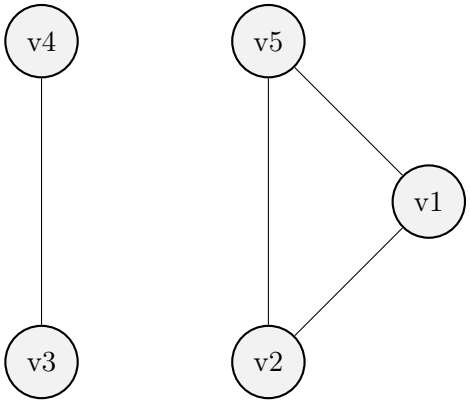


Figure 0.5: Not A Connected Graph

Strong Connectivity

A directed graph is a strongly connected graph if there is a directed path from any node to any other node. Figure 0.6 shows a depiction of such a graph. Conversely, the graph depicted by figure 0.7 is not strongly connected.

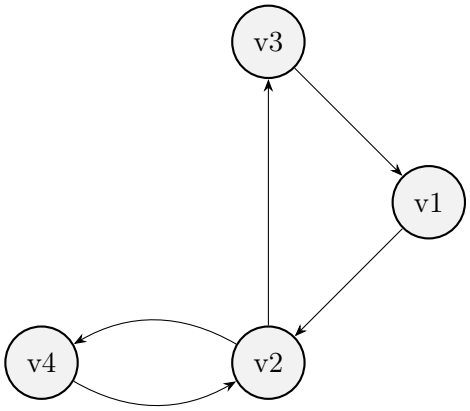


Figure 0.6: A Strongly Connected Graph

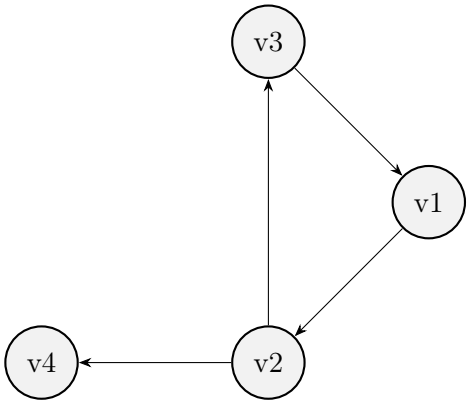


Figure 0.7: Not A Strongly Connected Graph

Transitive Closure

Given a digraph G, the Transitive Closure of G is the digraph G^* such that:

- G^* has the same vertices as G
- If G has a directed path from u to v ($u \neq v$), G^* has a directed edge from u to v.

Figure 0.8 shows a depiction of a transitive close of G.

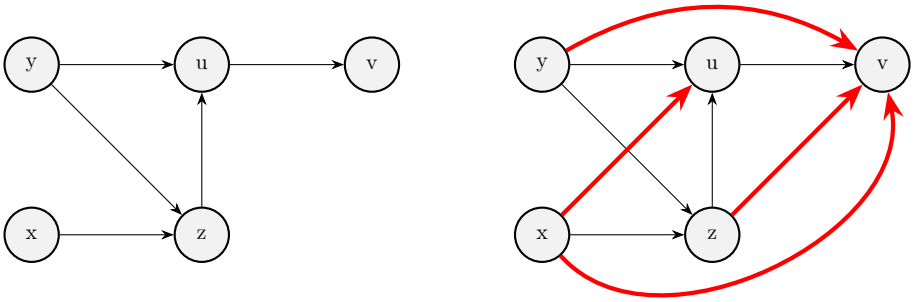


Figure 0.8: Transitive Closure

7.107 The degree sequence of a graph

Terminology - Undirected Graphs

Degree ($deg(v)$) the number of edges **incident** on v

- A loop contributes **twice** to the degree
- An isolated vertex has degree 0

In figure 0.9, we show a graph with the degree for every node written inside the node.

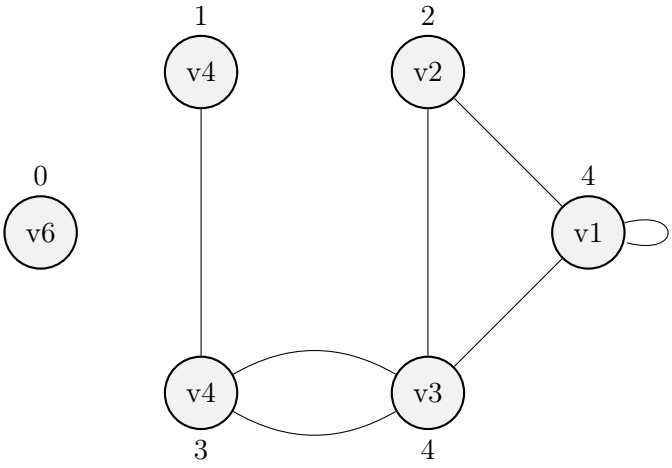


Figure 0.9: A graph with its vertices' degrees

Terminology - Directed Graphs

In-degree ($in - deg(v)$) Number of edges going **into** v

Out-degree ($out - deg(v)$**)** Number of edges going **out of** v

Degree ($deg(v)$**)** $out - deg(v) + in - deg(v)$

In figure 0.10 we show a graph with all in and out degrees for every vertex.

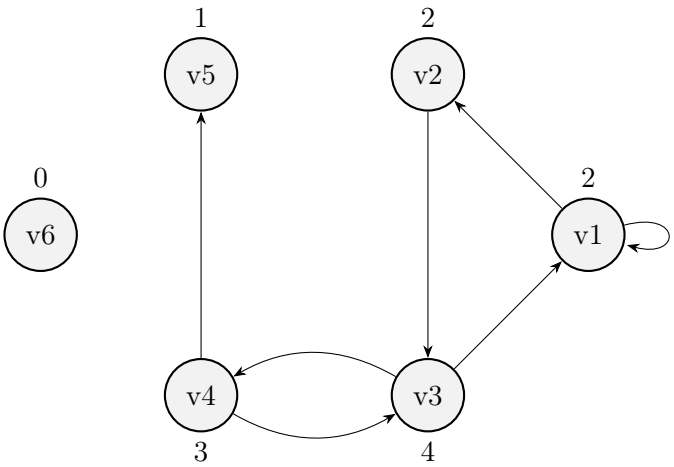


Figure 0.10: A digraph with its vertices' degrees

Degree sequence of a graph

Given an undirected graph G, a degree sequence is a monotonic non-increasing sequence of the vertex degrees of all the vertices of G.

The degree sequence of the graph from figure 0.11 is **4,3,2,1**.

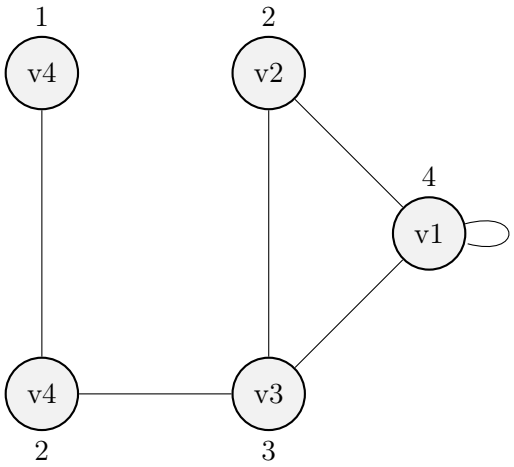


Figure 0.11: A graph with its degree sequence

Degree sequence property I

- The sum of the degree sequence of a graph is always even

Degree sequence property II

- The sum of the degree sequence of a graph is always twice the number of edges

7.109 Special graphs: simple, r-regular and complete graphs

Simple Graphs

A graph which contains no loops and no parallel edges, like the one in figure 0.12.

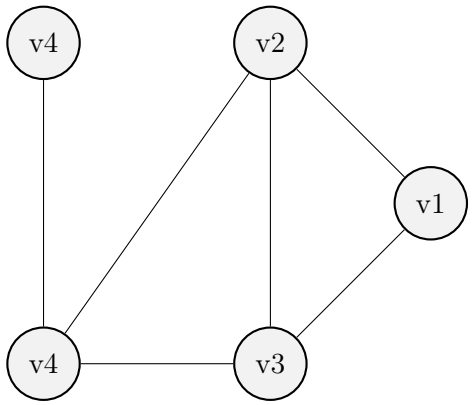


Figure 0.12: Simple graph

Properties of simple graphs

- Given a simple graph G with n vertices, the degree of each vertex of G is at most $n-1$

Regular graphs

A graph is said to be regular if all local degrees are the same number.

A graph G where all vertices have the same degree r is called an r-regular graph.

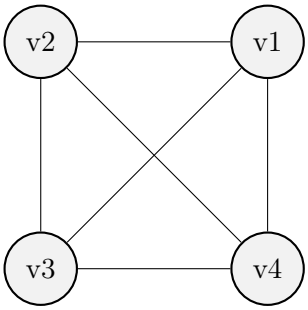


Figure 0.13: 3-regular graph

Properties of regular graphs

Given an r-regular graph G with n vertices, the following is true:

- Degree sequence of G is $r, r, r, \ldots$ (repeated n times)
- Sum of degree sequence is $r \cdot n$
- Number of edges in G is $\frac{r \cdot n}{2}$

Complete graph

A simple graph where every pair of vertices is adjacent. Complete graphs with n vertices are represented by the symbol K_n.

Figure 0.14 shows an example of a complete graph with 8 vertices.

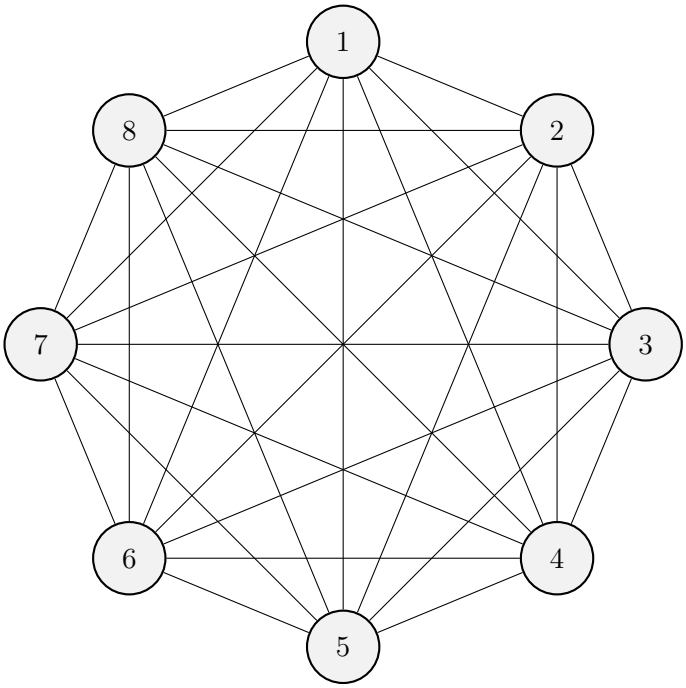


Figure 0.14: Complete graph

Complete graph properties

A complete graph with n vertices, K_n has the following properties:

- Every vertex has degree $n-1$
- Sum of degree sequences is $n(n-1)$
- Number of edges is $\frac{n(n-1)}{2}$

Week 14

Learning Objectives

- Define the adjacency matrix of a graph.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.632–636, pp.643–650, pp.652–663 and pp.681–688.
- Exercises

  pp.641–642 exercises 17–23

  pp.650–652 exercises 1–4, 6–18, 22–24 and 40–44

  pp.663–664 exercises 1–3, 7, 16 and 17

  pp.688–689 exercises 2–5, 13 and 14.

7.201 Isomorphic graphs

Definition of isomorphism

Two graphs G_1 and G_2 are isomorphic if there is a bijection (an invertible function) $f : G_1 \to G_2$ that preserves adjacency and non-adjacency.

This means that if uv is an edge in G_1, then $f(u)f(v)$ is an edge in G_2. In other words, u and v are adjacent in G_1 if and only if $f(u)$ and $f(v)$ are adjacent in G_2.

Properties of isomorphic graphs

- Two graphs with different degree sequences cannot be isomorphic
- Two graphs with the same degree sequence aren't necessarily isomorphic

7.203 Bipartite graphs

A graph $G(V, E)$ is called bipartite if the set of vertices V can be partitioned in two disjoint sets V_1 and V_2 such that edge e in G has one endpoint in V_1 and one endpoint in $V2$.

Figure 0.1 depicts a bipartite graph:

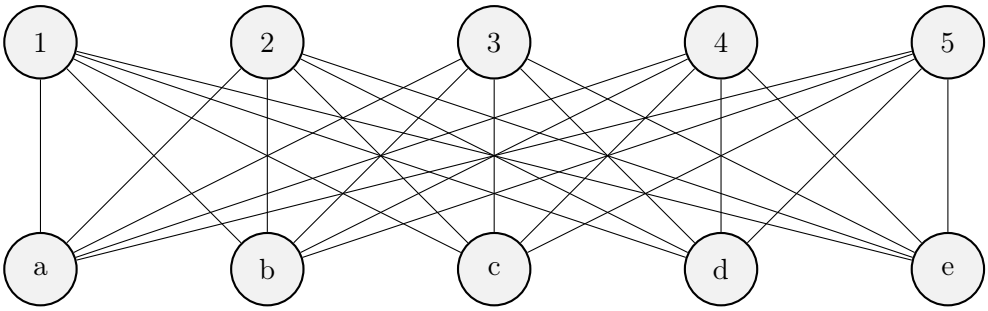


Figure 0.1: Bipartite Graph

Bipartite graphs are 2-colourable, meaning 2 colours are enough to color the graphs in a way that adjacent nodes do not have the same colour.

There are no odd-length cycles in bipartite graphs.

Matching

A Matching is a set of pairwise non-adjacent edges, none of which are loops. Meaning no two edges share the same endpoint.

A vertex is matched (or saturated) if it is an endpoint of one of the edges in the matching. Otherwise, the vertex is unmatched.

Maximum matching

A matching of maximum size such that if any edge is added, it is no longer a matching.

In a single bipartite graph, there may be many possible maximal matchings.

The Hopcroft-Karp Algorithm 1

The Hopcroft-Karp Algorithm is an algorithm for finding the maximum matching in a bipartite graph.

Augmenting paths a path that starts on a free node, ends on a free node and alternates between unmatched and matched edges within the path

Breadth First Search traversing the graph level by level

Depth First Search traversing the graph all the way to the leaf before starting another path

A simplified pseudocode for the algorithm is as follows:

1. $M \leftarrow \emptyset$
2. While there is an augmenting path P
   a) Use BFS to build layers that terminate at free vertices
   b) Start at free vertices in C, use DFS
3. Return M

7.205 The adjacency matrix of a graph

- Adjacency list
- Adjacency matrix
- Properties of adjacency matrix

Graph representation recap

Graphs can be represented as a set of vertices and a set of edges.

Adjacency list

A list of all the vertices of G and their corresponding individual adjacent vertices. Table 0.1 shows the adjancency list for the graph in figure 0.2.

Table 0.1: Adjancency list

Vertex	Adjacent Vertices
A	B, C
B	A, C, D
C	A, B, D, E
D	B, C, E
E	C, D

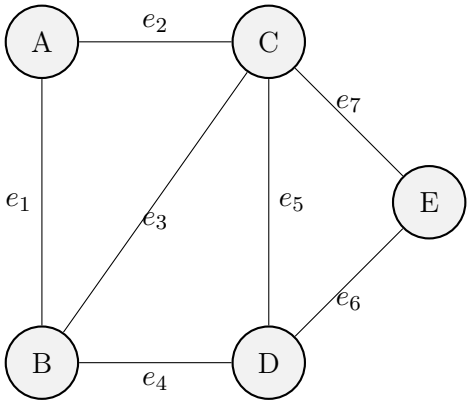


Figure 0.2: Sample Graph For Adjacency List

Note that we can draw a graph from its adjacency list alone.

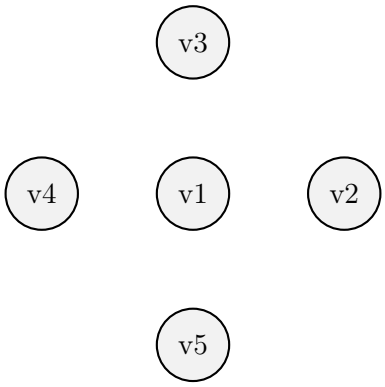
Example

Given the adjacency list in table 0.2, let's draw the graph:

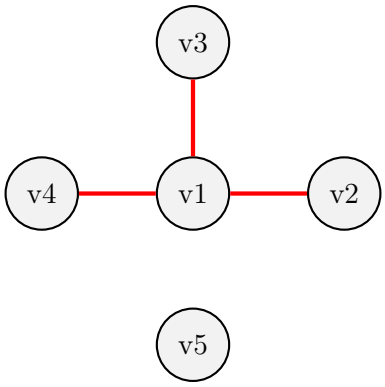
Table 0.2: Adjancency list

Vertex	Adjacent Vertices
v_1	v_2, v_3, v_4
v_2	v_1
v_3	v_1, v_4, v_5
v_4	v_1, v_3, v_5
v_5	v_3, v_4, v_5

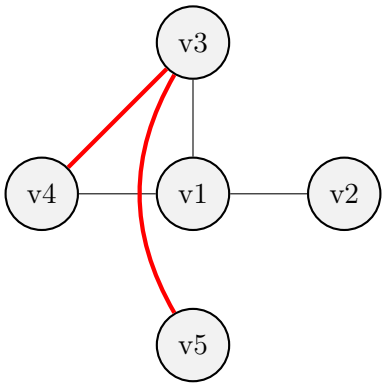
We know, from table 0.2 that the graph has 5 vertices. So we can start our drawing with only 5 vertices drawn, without any edges. That's shown below:



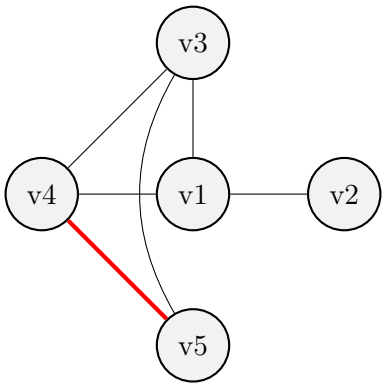
Now we can start adding edges. First covering v_1's adjacent vertices:



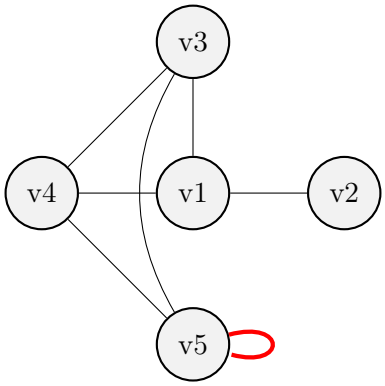
Next we go for v_2, but that's already covered. So we move on to v_3:



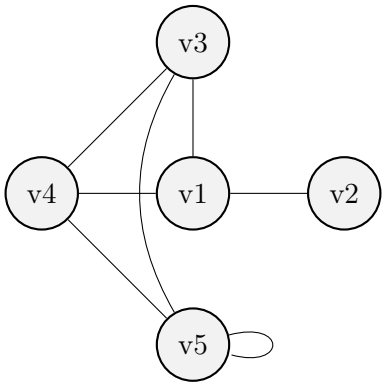
Next, we tackle for v_4:



Lastly, we look at v_5:



Now that all vertices are done, the final graph is:



Adjacency matrix

A graph can be represented by its adjacency matrix. Given the graph is figure 0.3, we can produce its adjacency matrix as shown below:

$$M(G) = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 0 \end{bmatrix}$$

The format of the matrix is as follows:

$$M(G) = \begin{bmatrix} v_1v_1 & v_1v_2 & v_1v_3 \\ v_2v_1 & v_2v_2 & v_2v_3 \\ v_3v_1 & v_3v_2 & v_3v_3 \end{bmatrix}$$

Note that in the leading diagonal, we have the loops which are counted twice. One interesting observation is that sum of all the edges in the undirected graph, is equal to

half the sum of all the elements in its adjacency matrix. The sum of the degree sequence is equal to the sum of the adjacency matrix.

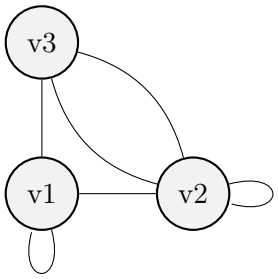


Figure 0.3: A graph for producing adjacency matrix

The adjacency matrix can also be produced for a directed graph, but we need to in mind that v_1 being adjacent to v_2 does not imply v_2 being adjacent to v_1.

7.207 Dijkstra's algorithm

Weighted graphs

A weighted graph is a graph in which each edge is assigned a weight. Like shown in figure 0.4.

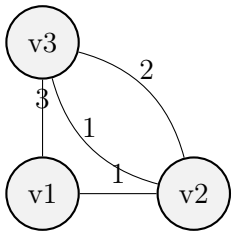


Figure 0.4: Weighted Graph

It can be used to model the distance between cities, response time in a network or the cost of a transaction, among other things.

Dijstra's algorithm

In 1956, Edsger Dijkstra designed an algorithm for finding the shortest path between any two nodes in a weighted graph. This algorithm is now know as Dijkstra's Algorithm.

Week 15

Learning Objectives

- Define a tree.
- Define spanning trees.
- Define non-isomorphic spanning trees.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.715–717, pp.753–762 and pp.764–769.
- Exercises

  p.725 exercises 1 and 11

  p.763 exercises 1–3, 5 and 6

  p.769 exercises 1–5.

8.103 Definition of a tree

Acyclic graph

A graph G is acyclic if and only if it has no cycles.

Definition of a tree

A tree is a connected acyclic undirected graph. Figure 0.1 depicts a sample tree. A tree cannot have loops or parallel edges.

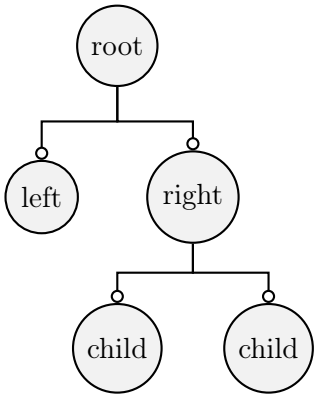


Figure 0.1: A sample tree

Definition of a forest

A forest is a cycle-free disconnected graph.

Theorem 1

An undirected graph is a Tree if and only if there is a unique simple path between any two of its vertices.

Well, if there are more than one path, we have a cycle.

Theorem 2

A tree with n vertices has $n - 1$ edges.

Rooted trees

A Rooted Tree is a tree in which one vertex has been designated as the **root**. Every edge is directed away from the root.

8.105 Spanning trees of a graph

A spanning tree of a graph G, is a connected subgraph of G that contains all vertices of G, without any cycles.

Figure 0.2 shows a complete graph with 4 vertices:

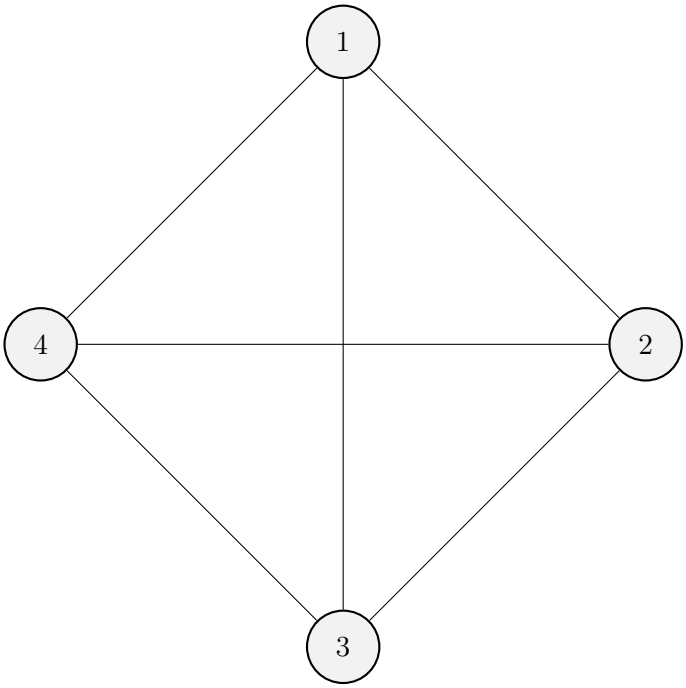


Figure 0.2: Complete graph with 4 vertices

There are four possible spanning trees in this graph.

Constructing a spanning tree

To get a spanning tree of graph G

1. Keep all vertices of G
2. Break all the cycles but keep the tree connected

Figures 0.3, 0.4, 0.5 show the process in a visual form. Note that figure 0.5 shows one out of 16 possible spanning trees for the graph shown in figure 0.3.

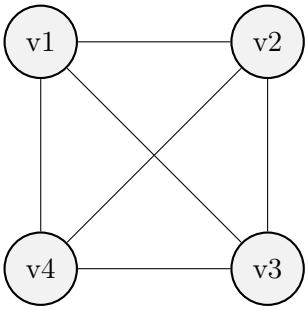


Figure 0.3: Starting Graph G

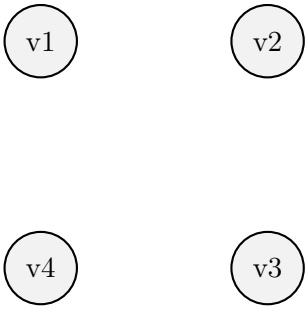


Figure 0.4: Keep all the vertices

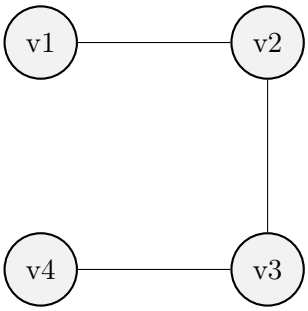


Figure 0.5: Break all cycles but keep the tree connected

Non iso-morphic spanning trees

Two spanning trees are said to be iso-morphic if there is a bijection preserving adjacency between the two trees.

8.107 Minimum spanning tree

Spanning tree cost

Suppose we have a connected undirected graph with a weight (or cost) associated with each edge. The cost of a spanning tree would be the sum of the cost of its edges.

The cost of the spanning tree marked in red is $8 + 3 + 2 + 1 = 14$.

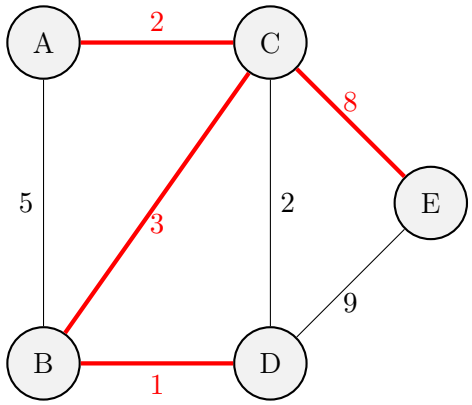


Figure 0.6: Sample Graph With Weights

Minimum-cost spanning tree

A spanning tree with the lowest cost.

Finding spanning trees

There are two basic algorithms for finding minimum-cost spanning trees.

- Kruskal's Algorithm
- Prim's Algorithm

Both are greedy algorithms.

Week 16

Learning Objectives

- Define minimum spanning trees.
- Define rooted trees and binary trees, and find the height of binary trees.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.717–725 and pp.726–729.
- Exercises

  p.725–726 exercises 2–8, 12, 13, 24 and 26

  p.738 exercises 1–4.

8.201 Rooted trees

Definition of a rooted tree

A Rooted Tree is a tree in which a vertex r has been designated the root of the tree. For every other vertex v there is a directed path to r.

The edges of a rooted tree are either away from the root (arborescence or out-tree) or towards the root (anti-arborescence or in-tree).

Figure 0.1 shows the depiction of a rooted tree:

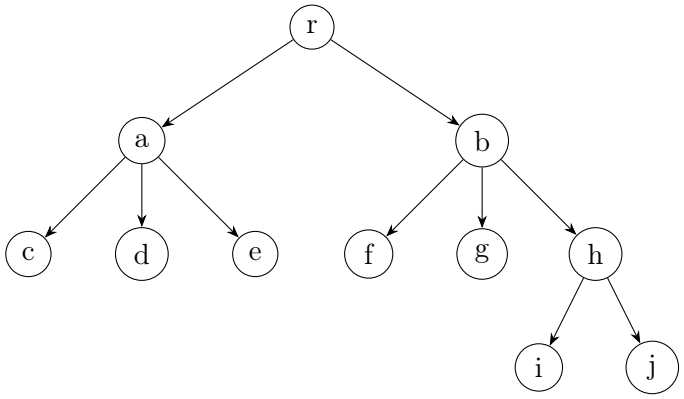


Figure 0.1: Rooted Tree

Theorem

A directed tree is a rooted tree if and only if one vertex has in-degree 0 and all the other vertices have in-degree 1.

Terminology of rooted trees

Using figure 0.1 as an example, we have:

- r is the root of the tree
- a is the parent of vertices c, d, e
- f, g, h are the children of b
- r and b are ancestors of i and j
- i and j are sibblings
- h and b are internal nodes
- c, d, e, f, g, i, j are external nodes

Depth and height in a tree

The depth (or path length) of a node in a tree is the number of edges between that node and the root. With regards to figure 0.1, we can say:

- depth of r is 0
- depth of a and b is 1
- depth of c, d, e, f, g, h is 2
- depth of i and j is 3

The height of a node in a tree is the **longest** from that node to a leaf.

- height of r is 3
- height of b is 2
- height of a and h is 1
- height of c, d, e, f, g, i, j is 0

The depth or height of a tree is the maximum path length across all its nodes. The height of the graph in figure 0.1 is 3.

Special trees

Binary Tree A tree in which every vertex has 2 or fewer children

Ternary Tree A tree in which every vertex has 3 or fewer children

m-ary Tree A tree in which every vertex has m or fewer children

Regular rooted trees

An m-ary tree is regular if every one of its internal nodes has exactly m children.

Properties

- An m-ary tree has at most m^h vertices at level h

Isomorphic trees

Two trees T_1 and T_2 are isomorphic if there is a bijection:

$$f : V(T_1) \to V(T_2)$$

which preserves **adjacency** and **non-adjacency**. This means that if uv is in $E(T_1)$ then $f(u)f(v)$ is in $E(T_2)$.

Notation $T_1 \cong T_2$ means T_1 and T_2 are isomorphic.

Properties

- Two trees with different degree sequences are not isomorphic
- Two tree with **the same** degree sequence are not **necessarily** isomorphic

Isomorphic rooted trees

Two isomorphic trees are isomorphic as rooted trees if and only if there is a bijection that maps the root of one tree to the root of another tree.

Properties

Two trees which are isomorphic may or may not be isomorphic as rooted trees.

8.203 binary search trees

Definition

a Binary Search Tree (BST) is a rooted binary tree whose internal nodes stores keys and, optionally, an associated value. The tree also satisfies the Binary Search property which requires that the key in each node must be greater than or equal to the keys in the nodes on the left subtree and less than or equal to the keys in the nodes on the right subtree.

Example

The tree depicted by figure 0.2 is a Binary Search Tree.

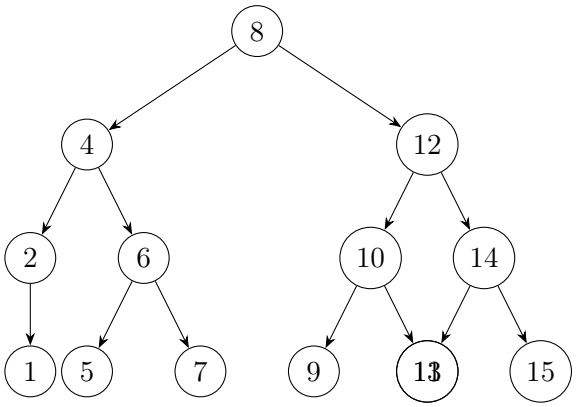


Figure 0.2: Binary Search Tree

Applications

BST are good data stores for modifiable data. It allows very fast insertion, deletion and searching.

Height of the tree

There are two methods to find the height of a tree with n elements.

The first method employs a $\log_2$ inequality:

$$2^{h-1} < n + 1 \leq 2^h$$
$$h - 1 < \log_2(n + 1) \leq h$$

While the second method relies on the ceiling function:

$$h = \lceil \log_2(n + 1) \rceil$$

It should be clear that both of these will give the same result and are equivalent.

Binary search algorithm

Start by comparing the midpoint. The list is then split into two sub-lists of approximately the same size.

The search is restricted to the appropriate sub-list based on the comparison of the midpoint.

This process continues until the element we're looking for is found or the list has be completely consumed.

Week 17

Learning Objectives

- Define a relation.
- Define a relation digraph.
- Describe the properties of a relation.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.553–561
- Exercises

  p.561 exercises 1–12

  p.562 exercises 20-22

9.101 Introduction

A binary relation over two sets A and B is a subset of the Cartesian product $A \times B$. We say that the element a of A is related to the element b of B, if and only if the ordered pair (a, b) is belongs to the set.

This same idea can be extended to more than two sets by considering the cartesian product with rank k. Instead of an ordered pair, we would have k-tuples. The relation in this case is referred to as finitary relation or n-ary relation.

In mathematics we study relationships such as:

- Relation between a positive integer and one it divides
- Relation between a real number and one larger than it
- Relation between a real number x and the value $f(x)$, where f is a function

9.103 Definition of a relation: relation versus function

What is a relation?

A relation can be defined between elements of a set B and elements of another set B. It can also be defined between elements of the same set.

We always refer to a relation by the letter R.

More formally, let A and B be two sets. Let R be a relation linking elements of the set A to elements of the set B. Let $x \in A$ and $y \in B$. We say that x is related to y with respect to the relation R and write $x\ R\ y$.

A relation is a link between two elements of a set. For example person x is a **SON OF** a person y. Where **SON OF** is a relation that links x to y.

When x is the son of y, we write $x\ R\ y$. When x is **not** the son of y, we write $x \not R x$.

Cartesian product

If we have two sets A and B, as depicted below:

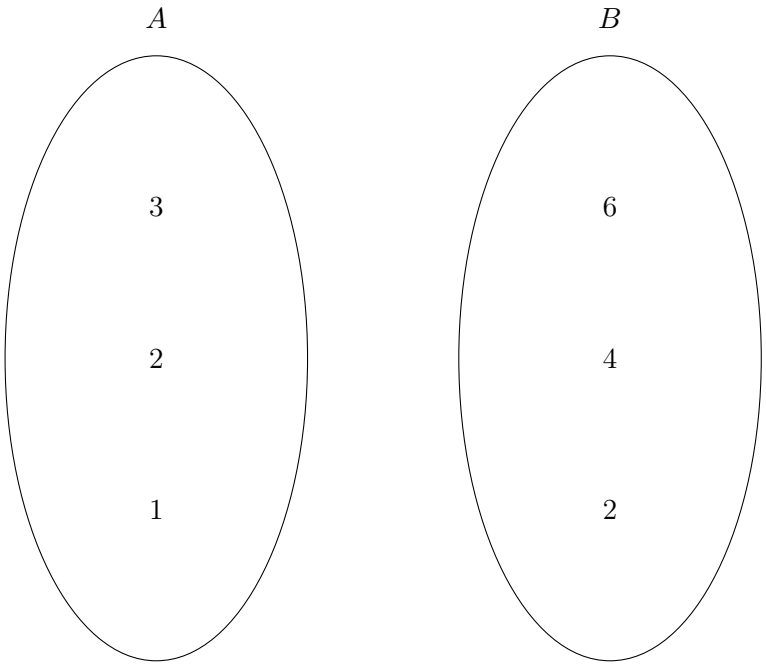


Figure 0.1: Sets A and B

The Cartesian Product $A \times B$ is defined by a set of ordered pairs (a, b) where $a \in A$ and $b \in B$.

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

For example, from our sets A and B shown in figure 0.1, we have:

$$A \times B = \{(1, 2), (1, 4), (1, 6), (2, 2), (2, 4), (2, 6), (3, 2), (3, 4), (3, 6)\}$$

Definition of relation

A binary relation over two sets A and B is a subset of the Cartesian product $A \times B$. In other words, $R \subseteq A \times B$. This means that R is the set of ordered pairs (a, b) where $a \in A$ and $b \in B$.

$(a, b) \in R$ means $a \; R \; b$.

Relations on a set

When $A = B$, we have a relation from A to A, or $R \subseteq A \times A$.

Example

Let $A = \{1, 2, 3, 4\}$. Let R be a relation on A.

$x, y \in A$, $x \; R \; y$ if and only if $x < y$. Therefore: $1 \; R \; 2$, $1 \; R \; 3$, $1 \; R \; 4$, $2 \; R \; 3$, $2 \; R \; 4$, $3 \; R \; 4$. We can see that $R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$.

9.105 Matrix and graph representations of a relation

Relations using matrices

Given a relation R from A to B we should list the elements of A and B. Ordering doesn't matter, however, it's conventional to list elements in ascending order.

Let $n_a = |A|$ and $n_b = |B|$, we can produce a matrix M_r of dimensions $n_a \times n_b$ such that:

$$m_{ij} = \begin{cases} 1 & \text{if} (a_i, b_j) \in R \\ 0 & \text{if} (a_i, b_j) \notin R \end{cases}$$

Example

Let $A = \{\text{Sofia}, \text{Samir}, \text{Sarah}\}$ and \$B = \ CS100, CS101, CS102, CS103\. Consider the relation of who's enrolled in which class defined in the table below:

	CS100	CS101	CS102	CS103
Sofia	X	X		
Samir		X	X	
Sarah	X		X	

We can produce a matrix representation of this relation as follows:

$$A_{m,n} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Combining relations

Union The union of two relations is the same as the union of two sets as defined in section Union ($\cup$). The union produces a new set containing all ordered pairs that are in at least one relation. The union of two relations R and $\mathcal{S}$ is written as $R \cup \mathcal{S}$ or R or$\mathcal{S}$

Intersection Works the same as defined in section Intersection ($\cap$). Contains all the elements that are in both R and $\mathcal{S}$. Written as $R \cap \mathcal{S}$ or R and$\mathcal{S}$

Combining relations via Boolean operators

Let:

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

and

$$M_{\mathcal{S}} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

The union (join) of these two relations can be calculated as:

$$M_{R \cup \mathcal{S}} = M_R \vee M_{\mathcal{S}} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

The intersection (meet) of these two relations can be calculated as:

$$M_{R \cap \mathcal{S}} = M_R \wedge M_{\mathcal{S}} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Representing relations using directed graphs

When a relation is defined on a set, it can be represented by a digraph.

In order to build a digraph for a relation on a set A, we follow these steps:

1. List all elements of A
2. When $(a, b) \in R$, a directed edge from a to b is drawn
3. Repeat until all ordered pairs (a, b) are drawn

Example

Let $A = \{1, 2, 3, 4\}$, let $R = \{(x, y) \mid x|y\}$. The relation R can be represented by the digraph below:

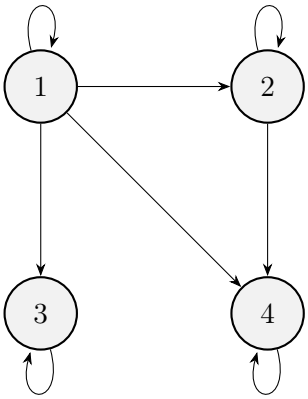


Figure 0.2: A digraph representation of relation R

9.107 The properties of a relation: reflexive, symmetric and anti-symmetric

Definition of reflexivity

A relation R in a set S is said to be reflexive if and only if $x \; R \; x, \forall x \in S$. This means that $(x, x) \in R$.

Example

Let R be the relation:

$$R = \{(a, b) \in \mathbb{Z}^2 \mid a \leq b\}$$

It's easy to see that this relation is reflexive. Well take any arbitrary element x in $\mathbb{Z}$, we can show that $x \leq x$, which means $x\ R\ x$, hence $(x, x) \in R$.

This implies that this relation R is **reflexive**.

Conversely, the relation:

$$R = \{(a, b) \in \mathbb{Z}^2 \mid a < b\}$$

Is **not** reflexive because $x \not< x$, hence $x \not R x$.

Digraph of reflexive relation

Every node in the digraph will have a loop, as shown in figure 0.3

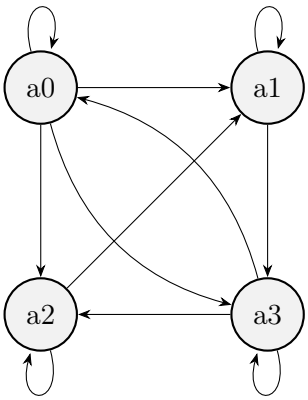


Figure 0.3: Reflexive Relation

Matrix of a reflexive relation

When looking at the matrix M_R of a reflexive relation R, all elements of the main diagonal will be 1, as shown below:

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Definition of symmetry

A relation R in a set S is symmetric if and only if $\forall a, b \in S, a\ R\ b \rightarrow b\ R\ a$.

Digraph of a symmetric relation

The digraph of a symmetric relation contains a symmetric pair of arcs or every edge of S. This is depicted in figure 0.4.

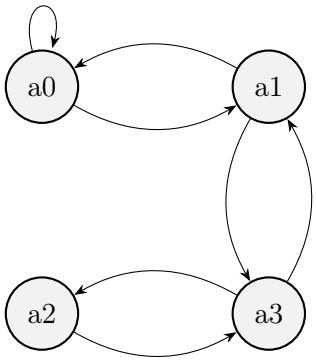


Figure 0.4: Symmetric Relation

Matrix of symmetric relation

The matrix M_R of a symmetric relation is, itself, symmetric. As shown below:

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Definition of anti-symmetric

A relation R is anti-symmetric if and only if $\forall a, b \in S, (a \ R \ b \wedge b \ R \ a) \rightarrow a = b$.

Digraph of anti-symmetric relation

The digraph of an anti-symmetric relation contains **no** parallel edges between any two different vertices. As depicted in figure 0.5.

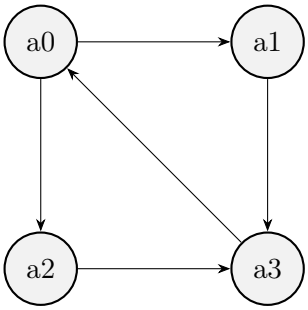


Figure 0.5: Anti-symmetric Relation

Matrix of anti-symmetric relation

Let M_R be the matrix of an anti-symmetric relation. If $i \neq j$ and $m_{ij} \neq 0$, then $m_{ji} = 0$.

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

9.109 Relation properties: transitivity

Definition of transivity

A relation R on a set S is called transitive if and only if $\forall a, b, c \in S, (a \ R \ b \wedge b \ R \ c) \rightarrow a \ R \ c$.

Examples

1. R= $\{(x, y) \in \mathbb{N}^2 \mid x \leq y\}$

   Transitive if $x \leq y$ and $y \leq z$, then $x \leq z$.

2. R= $\{(2, 3), (3, 2), (2, 2)\}$

   Not Transitive $3 \ R \ 2$ and $2 \ R \ 3$ but $3 \not R 3$

Transitive closure of a relation

Given the relation depicted in figure 0.6, what is the minimum number of edges to make the relation transitive?

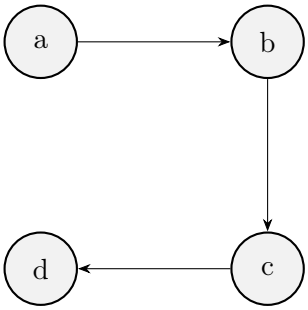


Figure 0.6: Initial Relation

We can see that $a\ R\ b$ and $b\ R\ c$ but $a \not R c$, therefore we must add a new edge from a to c, as depicted in figure 0.7.

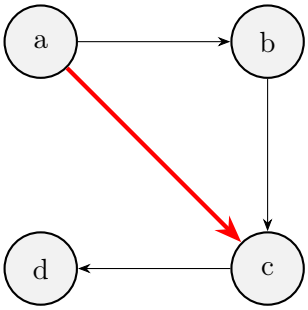


Figure 0.7: First new edge

We can also see that $b\ R\ c$ and $c\ R\ d$, but $b \not R d$, therefore we must add a new edge from b to d.

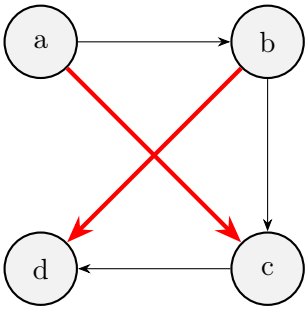


Figure 0.8: Second new edge

This relation is still not transitive. When we added the new edge depicted in figure 0.7, we created a new situation where $a\ R\ c$ and $c\ R\ d$ but $a \not R d$, therefore we must add a new edge from a to d.

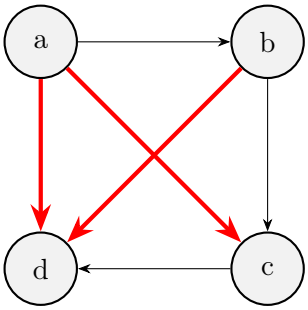


Figure 0.9: Final new edge

Finally, we have a transitive relation which is called the **Transitive Closure** of the original relation R.

Week 18

Learning Objectives

- Define an equivalence relation.
- Define partial and total order.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.570–575, pp.587–594 and pp.597–601.
- Exercises

  pp.575–576 exercises 1–4 and 14–22

  pp.594–595 exercises 1–6, 9, 17–23, 25 and 32

  p.609 exercises 1, 5–7 and 12–15.

9.201 Equivalence relations and equivalence classes

Definition of equivalence relation

Equivalence Relations are binary relations that are reflexive, symmetric, and transitive.

Example

Let R be a relation of elements in $\mathbb{Z}$:

$$R= \{(a,b) \in \mathbb{Z}^2 \mid a \mod 2 = b \mod 2\}$$

This relation is:

Reflexive $a\ R\ a, \forall a \in \mathbb{Z}$

Symmetric $\forall a, b \in \mathbb{Z} a\ R\ b \rightarrow b\ R\ a$

Transitive $\forall a, b, c \in \mathbb{Z}(a\ R\ b \wedge b\ R\ c) \rightarrow a\ R\ c$

$\therefore R$ is an equivalence relation.

Definition of equivalence classes

An equivalence class is a subset of a set S such that equivalent elements are part of that subset.

In order words, if the elements of S have a notion of equivalence (by means of an equivalence relation R) defined on them, then we can split the set S into equivalence classes in such a way that elements a and b belong to the same equivalence class (a subset of S) if and only if a and b are equivalent.

This means that the equivalence class defined by the equivalence relation R will form a subset of S containing all elements **related to** a through R.

Formally, it's defined as follows:

$$[\text{a}] = \{x : x \in S \mid x \; R \; a\}^1$$

Example

Let $S = \{1, 2, 3, 4\}$ and R be a relation on elements in S:

$$R = \{(a, b) \in S^2 \mid a \mod 2 = b \mod 2\}$$

R is an equivalence relation with 2 equivalence classes:

- $[1] = [3] = \{1, 3\}$
- $[2] = [4] = \{2, 4\}$

Graphically:

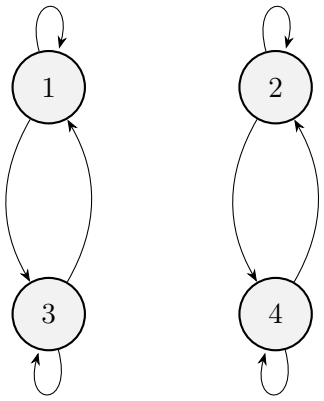


Figure 0.1: Two equivalence classes

[1] In Rosen's book, the notation $a \backsim b$ is used instead of $a \; R \; b$

9.203 Partial and total order

Definition of partial order

If we have a relation R, we say that R is a Partial Order if and only if R is:

- Reflexive
- Anti-symmetric
- Transitive

Example

Let R be a relation of elements in $\mathbb{Z}$

$$R= \{(a,b) \in \mathbb{Z}^2 \mid a \leq b\}$$

This relation is:

Reflexive $\forall a \in \mathbb{Z} a \leq a$

Transtivie $\forall a,b,c \in \mathbb{Z}(a \leq b \wedge b \leq c) \rightarrow a \leq c$

Anti-symmetric $\forall a,b \in \mathbb{Z}(a \leq \wedge b \leq a) \rightarrow a = b$

$\therefore R$ is a partial order.

Definition of total order

If we have a relation R on the elements of a set S, we say that R is a Total Order if and only if R is:

- a partial order
- $\forall (a,b) \in S(a \ R \ b \vee b \ R \ a)$
  - this part means that every pair of elements in S must be comparable with respect to the relation R

Example

Let R be a relation of elements in $\mathbb{Z}$

$$R= \{(a,b) \in \mathbb{Z}^2 \mid a \leq b\}$$

This relation is:

- A partial order (see previous example)
- $\forall a,b \in \mathbb{Z}(a \leq b \vee b \leq a)$

Week 19

Learning Objectives

- Apply the addition principle and the multiplication principle to count objects when they are sampled with or without replacement.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.375–385 and pp.395–401.
- Exercises

  pp.386–387 exercises 1–5, 7, 8, 14–17, 30, 32 and 40

  pp.394–395 exercises 1–6, 14, 15, 19 and 28

  pp.402–403 exercises 1–10, 16, 17, 20, 21, 32 and 34.

10.101 Introduction

Combinatorics is a branch of Discrete Mathematics concerned with the study of finite or countable discrete structures. It's the study of collections or arrangements of objects. Combinatorics finds applications in computer science, economics, physics, and many other fields.

10.103 The basics of counting

Product Rule

To compute the number of different possible outcomes in a process, we can break it into two independent tasks.

If there are n different ways of executing the first task and m different ways of executing the second task, then there are $n \cdot m$ different possible outcomes to the process.

One way to think about this is that if there are n ways of executing the first task, for each of those n ways, there will be m different ways of executing the second process.

Product rule in terms of sets

Let A be a set of ways to complete the first task and B be a set of ways to complete the second task. If A and B are disjoint, then the number of ways of completing both tasks, can be represented by:

$$|A \times B| = |A| \cdot |B|$$

This means that the cardinality of the cartesian product of two sets, is the product of cardinality of each set.

Addition Rule

Let's assume that we have two independent tasks. Task 1 can be completed in n ways and task 2 can be completed in m ways. Because these tasks are independent (i.e. completing task 1 or not has no effect on task 2), the total number of ways of completing both tasks is $n + m$.

Example

Let's assume that a University has to choose either a staff member or a student to be a University representative. Let's also assume that there are 77 students and 10 staff members and nobody is both a student and a staff member. How many ways are there to choose a representative?

$$77 + 10 = 87$$

The sum rule in terms of sets

Let A be the set of ways of completing task 1 and B be the set of ways of completing task 2, where A and B are disjoint sets. The number of ways of completing either task 1 or task 2 can be represented by:

$$|A \cup B| = |A| + |B|$$

Combining the sum and product rules

Let's assume that a label in a programming language can be either a single letter or a letter followed by 2 digits. How many possible labels are there?

$$\begin{aligned} single\_letter + letter\_2\_digits &= 26 + (letters \cdot digits^2) \\ &= 26 + (26 \cdot 10^2) \\ &= 26 + (26 \cdot 100) \\ &= 26 + 2600 \\ &= 2626 \end{aligned}$$

Subtraction rule

Suppose a task can be done in either one of n_1 ways or one of n_2 ways. Then the total number of ways to do the task is $n_1 + n_2$ minus the number of ways common to the two different ways.

This is also known as the Pinciple of Inclusion-Exclusion.

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

Division rule

Suppose a task can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to w. Then this task can be done in $\frac{n}{d}$ ways.

In terms of sets, if the finite set A is the union of n pair-wise disjoint subsets each with d elements, then $n = \frac{|A|}{d}$.

In terms of functions, if f is a function from A to B, where both A and B are finite sets, and for every value $b \in B$ there are exactly d values $a \in A$ such that $f(a) = b$, then $|B| = \frac{|A|}{d}$.

10.105 The pigeonhole principle

See Fundamentals of Computer Science notes and Pigeonhole Principle in wikipedia.

10.107 Permutations and combinations

See Fundamentals of Computer Science notes and Permutations and Combinations on wikipedia

Week 20

Learning Objectives

- Calculate the number of permutations of length r chosen from a set of n objects.
- Demonstrate how to use combination formulae to count the number of unordered subsets of r objects taken from a set of n distinct objects.
- Distinguish between combinations and permutations.
- Apply the techniques learnt in new counting problems.

Essential Reading

- Rosen, K.H. Discrete mathematics and its applications. (New York: McGraw-Hill, 2012) 7th edition, pp.403–409, pp.410–419 and pp.422–425.
- Exercises

  pp.409–410 exercises 1–7 and 13–15

  pp.419–421 exercises 1–8, 27, 28, 30–32, 44 and 45.

  p.425 exercises 1–3.

10.201 Binomial coefficients and identities

Binomial expression

An expression consisting of two terms connected by a $+$ or $-$ is a binomial expression.

For example

- $x + a$
- $2x - y$
- $x^2 + y^2$
- $3x - 2y$

Binomial theorem

The complexity of an expanded binomial expressions grows with the power.

$$\begin{aligned}(x+y)^1 &= x+y\\ (x+y)^2 &= x^2+2xy+y^2\\ (x+y)^3 &= x^3+3x^2y+3^xy^2+y^3\\ (x+y)^4 &= x^4+4x^3y+6x^2y^2+4xy^3+y^4\\ &\dots\end{aligned}$$

The Binomial Theorem states the following:

Let x and y be variables, and n a non-negative integer. The expansion of $(x+y)^n$ can be formalised as:

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

Example

What is the coefficient of x^8y^7 in the expansion of $(3x-y)^{15}$?

This expression can be re-written as $(3x+(-y))^{15}$. By the binomial theorem we can describe this expression as:

$$(3x+(-y))^n = \sum_{k=0}^{15} \binom{15}{k} (3x)^k (-y)^{15-k}$$

Therefore, we can set $k=8$ in order to find the coefficient. Which is:

$$\begin{aligned}\binom{15}{8} 3^8 (-1)^{15-8} &= \binom{15}{8} 3^8 (-1)^7\\ &= -3^8 \cdot \frac{15!}{8!7!}\end{aligned}$$

Pascal's identity

Pascal's identity helps us simplify complicated binomial coefficients.

It states that for positive natural numbers n and k:

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

Proof. Let T be a set where $|T| = n+1$, $a \in T$ and $S = t - \{a\}$.

There are $\binom{n+1}{k}$ subsets of T containing k elements. Each of these subsets either.

- contains a with another $k-1$ elements, or
- contains k elements of S and not a.

Hence, there are $\binom{n}{k-1}$ subsets of k elements containing a and $\binom{n}{k}$ subsets of k elements of T that don't contain a.

$\therefore \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$. □

Pascal's triangle

Using Pascal's identity, we can organise binomial coefficients in a trigular shape called Pascal's Triangle.

In this triangle, the element $a_{n,r}$ is the binomial coefficient $\binom{n}{r}$.

$n=0$:					$\binom{0}{0}$				
$n=1$:				$\binom{1}{0}$		$\binom{1}{1}$			
$n=2$:			$\binom{2}{0}$		$\binom{2}{1}$		$\binom{2}{2}$		
$n=3$:		$\binom{3}{0}$		$\binom{3}{1}$		$\binom{3}{2}$		$\binom{3}{3}$	
$n=4$:	$\binom{4}{0}$		$\binom{4}{1}$		$\binom{4}{2}$		$\binom{4}{3}$		$\binom{4}{4}$

We can also show the same triangle with coeffiecients pre-calculated, as follows:

$n=0$:					1				
$n=1$:				1		1			
$n=2$:			1		2		1		
$n=3$:		1		3		3		1	
$n=4$:	1		4		6		4		1

10.204 Generalised permutations and combinations

Permutations with repetition

The number of r-permutations of a set of n objects with repetition allowed is n^r.

Permutations without repetition

The number of r-permutations of a set of n objects without repetition allowed is $\dfrac{n!}{(n-r)!}$.

Combination with repetition

The number of ways in which k objects can be selected from n categories with repetition permitted is $\binom{n+k-1}{k} = \dfrac{(n+k-1)!}{k!(n-1)!}$.

Combination without repetition

The number of ways in which k objects can be selected from n categories without repetition permitted is $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.

Choice of formulas

	Ordered (permutations)	Unordered (combinations)
Repetition is not permitted	$\frac{n!}{(n-k)!}$	$\frac{n!}{k!(n-k)!}$
Repetition is permitted	n^k	$\frac{(n+k-1)!}{k!(n-1)!}$

10.206 Distinguishable objects and boxes

Counting problems can be phrased in terms of distributing k objects into n boxes.

Distinguishable objects and distinguishable boxes with exclusion

We want to distribute k balls, numbered from 1 to k, into n boxes, numbered from 1 to n, in such a way that no box receives more than one ball.

This is equivalent to making and ordered selection of k boxes from n boxes.