Discrete Mathematics Course Notes

Felipe Balbi

October 13, 2019

Week 1

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.

$$\begin{aligned} E &= \{2, 4, 6, 8\} \\ V &= \{a, e, i, o, u\} \\ EmptySet &= \{\} = \emptyset \end{aligned} \tag{1}$$

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:

$$A \subseteq B \iff \text{if x} \in A \text{then} x \in B (\text{for all x}) \tag{2}$$

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:

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

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

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

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*

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:

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

Example 2 What is the powerset of the empty set? What is the powerset of the powerset of the empty set?

$$\begin{aligned} P(\emptyset) &= \{\emptyset\} \\ P(P(\emptyset)) &= \{\emptyset, \{\emptyset\}\} \end{aligned} \tag{5}$$

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:

$$
\begin{aligned}
S &= \{1,2\} \\
|S| &= 2 \\
P(S) &= \{\emptyset, \{1\}, \{2\}, \{1,2\}\} \\
|P(S)| &= 4 = 2^2 = 2^{|S|}
\end{aligned} \tag{6}
$$

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

$$
\begin{aligned}
|P(A)| &= 2^n \\
|P(P(A))| &= 2^{2^n} \\
|P(P(P(A)))| &= 2^{2^{2^n}}
\end{aligned} \tag{7}
$$

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.*

$$A \cup B = \{x \mid x \in A \,\text{or}\, x \in B\} \tag{8}$$

Example

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

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.*

$$A \cap B = \{x \mid x \in A \,\text{and}\, x \in B\} \tag{10}$$

Example

$$\begin{aligned} A &= \{1,2,3\} \\ B &= \{2,3,4\} \\ A \cap B &= \{2,3,\} \end{aligned} \tag{11}$$

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.*

$$A - B = \{x \mid x \in A \,\text{and}\, x \notin B\} \tag{12}$$

Example

$$\begin{aligned} A &= \{1,2,3\} \\ B &= \{3,4,5\} \\ A - B &= \{1,2,\} \end{aligned} \tag{13}$$

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.*

$$A \oplus B = \{x \mid (x \in A \,\text{or}\, x \in B) \,\text{and}\, x \notin A \cap B\} \tag{14}$$

Example

$$\begin{aligned} A &= \{1,2,3\} \\ B &= \{3,4,5\} \\ A \oplus B &= \{1,2,4,5\} \end{aligned} \tag{15}$$

Membership Table ($A \oplus B$)

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

Summary

Operations

$$
\begin{aligned}
A &= \{1, 2, 3\} \\
B &= \{3, 4, 5\} \\
A \cup B &= \{1, 2, 3, 4, 5\} \\
A \cap B &= \{3\} \\
A - B &= \{1, 2\} \\
A \oplus B &= \{1, 2, 4, 5\}
\end{aligned}
\tag{16}
$$

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

1.201 The representation of a set using Venn diagrams

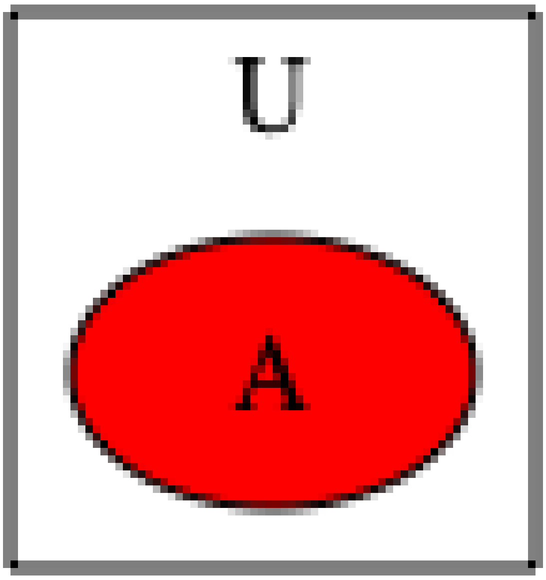
Venn diagrams can be used to represent sets and visualize the possible relations among a collection of sets. During this lesson we studied the following concepts:

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

The Universal Set

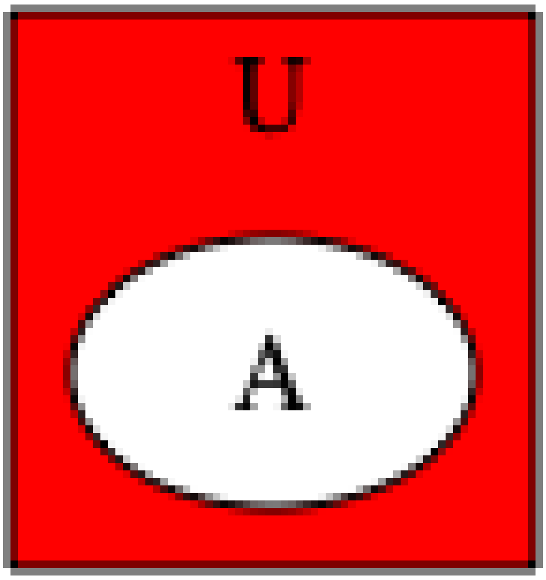
The universal set is a set containing everything. It's referred to by the letter `U`.

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

$$\begin{aligned}
U &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \\
A &= \{2, 4, 6, 8, 10\} \\
\overline{A} &= U - A \\
&= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} - \{2, 4, 6, 8, 10\} \\
&= \{1, 3, 5, 7, 9\}
\end{aligned} \tag{17}$$

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

$$A \cup \overline{A} = U \tag{18}$$

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

$$A \oplus B = A \cup B - (A \cap B) \tag{19}$$

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.

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \tag{20}$$

De Morgan's Second Law

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

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{21}$$

Proof using membership tables

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

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

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

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

$$2 + 3 = 3 + 2 \tag{22}$$

Same applies for multiplication:

$$2 \cdot 3 = 3 \cdot 2 \tag{23}$$

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

$$2 - 3 \neq 3 - 2 \tag{24}$$

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

$$\begin{aligned} A &= \{1, 2\} \\ B &= \{1, 3\} \\ A - B &= \{1, 2\} - \{1, 3\} = \{2\} \\ B - A &= \{1, 3\} - \{1, 2\} = \{3\} \\ (A - B) &\neq (B - A) \end{aligned} \tag{25}$$

Associativity

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

$$(a + b) + c = a + (b + c) \tag{26}$$

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

$$
\begin{aligned}
A &= \{1,2\} \\
B &= \{1,3\} \\
C &= \{2,3\} \\
(A-B)-C &= (\{1,2\}-\{1,3\})-\{2,3\} \\
&= \{2\}-\{2,3\} \\
&= \emptyset
\end{aligned}
\tag{27}
$$

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

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

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:

$$a \cdot (b+c) = a \cdot b + a \cdot c \tag{28}$$

Similarly, the set union is distributive over set intersection:

$$A \cup (B \cap C) = (A \cup B) \cap (B \cup C) \tag{29}$$

And the set intersection is distributive over the set union:

$$A \cap (B \cup C) = (A \cap B) \cup (B \cap C) \tag{30}$$

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

$$\begin{aligned}
\overline{(A \cap B) \cup \overline{B}} &= \overline{(A \cap B)} \cap \overline{\overline{B}} \\
&= \overline{(A \cap B)} \cap B \\
&= (\overline{A} \cup \overline{B}) \cap B \\
&= \overline{A} \cap B \cup \overline{B} \cap B \\
&= \overline{A} \cap B \cup \emptyset \\
&= \overline{A} \cap B \\
&= B \cap \overline{A}
\end{aligned} \tag{31}$$

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

During week 3 we learn the definition and properties of functions.

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:

$$\begin{aligned} S_1 &= \{Sea, Land, Sky\} \\ S_2 &= \{1, 2, 3, 4, 5, 6\} \\ \\ Sea &\rightarrow 3 \\ Land &\rightarrow 4 \\ Sky &\rightarrow 3 \end{aligned} \tag{32}$$

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 $f : A \rightarrow B$ and read as f maps A to B.*

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

Domain, co-domain and range of a function

Given a function $f : A \rightarrow B$

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

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:

$$\begin{aligned} On &\to 2 \\ Sea &\to 3 \\ Land &\to 4 \\ Sky &\to 3 \end{aligned} \tag{33}$$

In this case:

$$\begin{aligned} D_f &= A = \{On, Sea, Land, Sky\} \\ co - D_f &= B = \{1, 2, 3, 4, 5, 6\} \\ R_f &= \{2, 3, 4\} \end{aligned} \tag{34}$$

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.

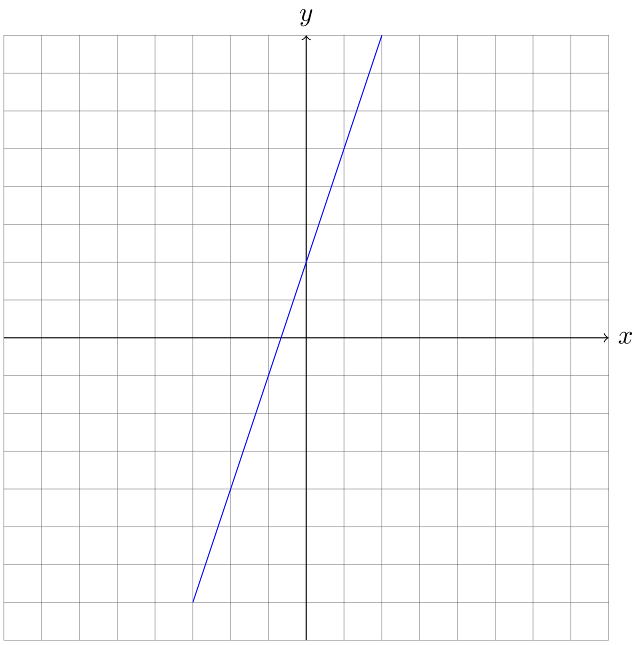
Linear Functions

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.

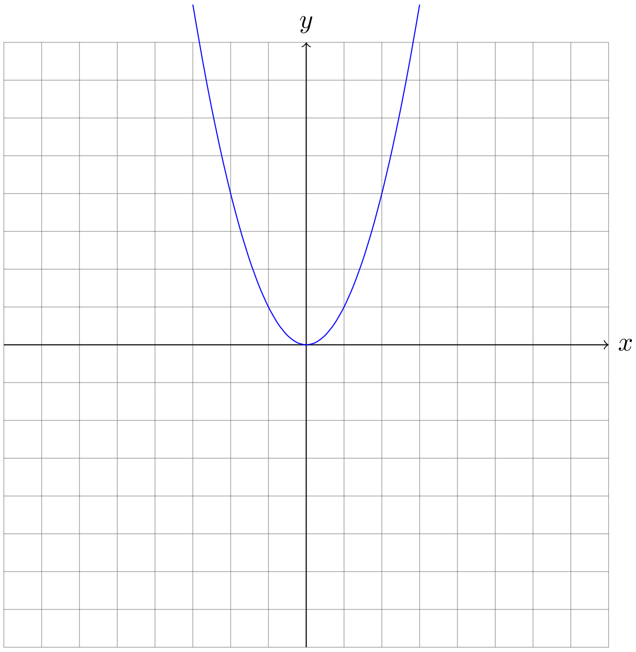
x	f(x)
0	2
1	5
2	8
3	11
4	14



Quadratic functions

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

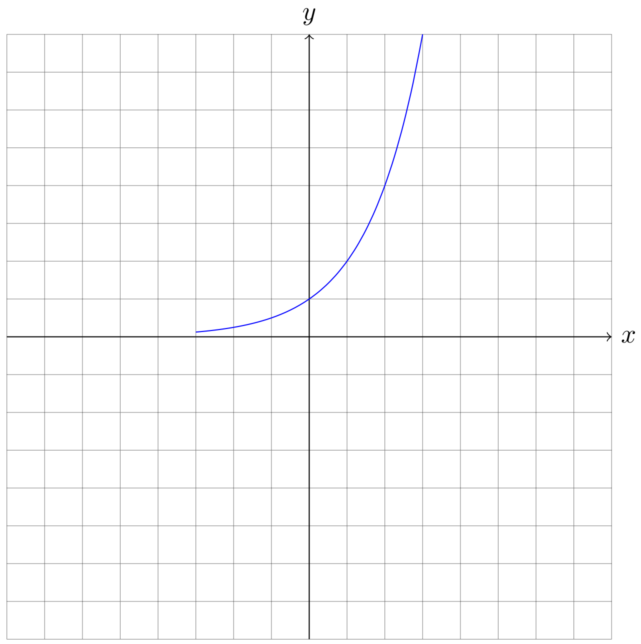
x	f(x)
0	0
1	1
2	4
3	9
4	16



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.

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}
$(b^x)^y$	$b^{x \cdot y}$
$(a \cdot b)^x$	$x^x \cdot b^x$
$\left(\frac{a}{b}\right)^x$	$\frac{a^x}{b^x}$
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. $\forall a, b \in A, f(a) = f(b) \implies a = b$

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 $a = b$.

$$\begin{aligned} f(a) = f(b) \implies & 2a + 3 = 2b + 3 \\ & 2a + 3 - 3 = 2b + 3 - 3 \\ & 2a = 2b \\ & \frac{2a}{2} = \frac{2b}{2} \\ & a = b \end{aligned} \tag{35}$$

$\therefore f$ is injective. □

The second proof assumes $a \neq b$

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

$$\begin{aligned} a \neq b \implies & 2a \neq 2b \\ & 2a + 3 \neq 2b + 3 \\ & f(a) \neq f(b) \end{aligned} \tag{36}$$

$\therefore f$ is injective. □

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.

$$\begin{aligned} f(5) = (5)^2 = (-5)^2 = f(-5) \\ \text{however}\, 5 \neq -5 \end{aligned} \tag{37}$$

$\therefore f$ 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. $R_f = co - D_f$).

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

$$\begin{aligned} f(x) = y \implies 2x + 3 = y \\ 2x + 3 - 3 = y - 3 \\ \frac{2x}{2} = \frac{y-3}{2} \\ x = \frac{y-3}{2} \in \mathbb{R} \end{aligned} \tag{38}$$

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

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. $\square$