UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 1 – Set theory and functions
Lecture 1.01 – Set notation

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Introduction to set theory and functions

The mathematical study of set theory began in 1874, founded by Georg Cantor. Mathematical sets underlie almost all branches of mathematics, and set theory provides an important framework for describing and understanding formal logic.

In MATH1081, we will encounter sets throughout all 5 topics of the course. In this first topic, we will also use sets to motivate the investigation of functions, another fundamental mathematical concept that appears in almost all branches of mathematics.

Much of our study of Topic 1 will be focused on definitions and results about sets and functions. Probably the most difficult part of this topic is understanding and applying the different methods of proof regarding properties of sets and functions. We will revisit these ideas in a more generalised sense in Topic 3 (Proofs and logic).

Set notation

Definition. A set is a well-defined, unordered collection of distinct objects. The objects contained in a set are called its elements.

Notation. A set can be represented by writing its elements surrounded by braces (curly brackets). For example, the set S with just the elements 1, 2, and 3 can be written as $S = \{1, 2, 3\}$.

Since sets are unordered collections, this set S can also be written as $S = \{3, 1, 2\} = \{1, 2, 3\}$.

Since the elements of a set are distinct, repetition of elements is ignored, so the set S can also be written as $S = \{1, 2, 2, 3, 3, 3\} = \{1, 2, 3\}$.

Example. Simplify each of the following sets.

- $\{x, a, y, x, a, y\} = \{a, x, y\}$.
- $\{\text{even numbers between 1 and 9}\} = \{2, 4, 6, 8\}$.
- $\{\text{letters in } \mathbf{BANANA}\} = \{\mathbf{A}, \mathbf{B}, \mathbf{N}\}$.

Notice that the elements of a set can be numbers, letters, or any other object, and can be given explicitly or descriptively.

Defining sets

Notation. The set membership symbol $\in$ is used to indicate that an object is an element of a set. We write $x \in S$ to mean "x is an element of S". We can also use the symbol $\notin$ to indicate non-membership of a set.

For example, writing $S = \{1, 2, 3\}$, we have $1 \in S$ but $0 \notin S$. Similarly, we have $a \in \{a, x, y\}$ while $b \notin \{a, x, y\}$.

We can properly define a set by writing out all its elements, or by giving a careful description of its elements. So long as there is no ambiguity, we can also use the ellipsis symbol ($\ldots$) to help describe a set. For example:

- $\{\text{letters in the English alphabet}\} = \{\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots, \mathbf{Z}\}$.
- $\{\text{positive even numbers}\} = \{2, 4, 6, 8, \ldots\}$.

Notation. A colon ($:$) or vertical bar ($|$) symbol can be used to introduce additional properties that define the elements of a set. We write

$$\{x \in S : (\text{some property of } x)\} \quad \text{or} \quad \{x \in S \mid (\text{some property of } x)\}$$

to mean "the set of elements in S that satisfy the property", or literally, "all x in S such that x satisfies the property".

For example, writing $S = \{1, 2, 3\}$, we have $\{x \in S \ : \ x > 1\} = \{2, 3\}$.

Numeric sets

Notation. The following are some important and commonly-used sets of numbers.

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, the set of natural numbers. Note here that $0 \in \mathbb{N}$.
- $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, the set of integers.
- $\mathbb{Z}^+ = \{x \in \mathbb{Z} \ : \ x > 0\} = \{1, 2, 3, \dots\}$, the set of positive integers.
- $\mathbb{Q} = \left\{\frac{p}{q} \ : \ p, q \in \mathbb{Z},\ q \neq 0\right\} = \left\{\frac{p}{q} \ : \ p \in \mathbb{Z},\ q \in \mathbb{Z}^+\right\}$, the set of rational numbers. The rational numbers include all integers and fractions.
- $\mathbb{R} = \{\text{all points on the real number line}\}$, the set of real numbers. The real numbers include all rational numbers as well as all irrational numbers like $\sqrt{2}$, π, and e.
- $\mathbb{C} = \{a + bi \ : \ a, b \in \mathbb{R},\ i^2 = -1\}$, the set of complex numbers. The complex numbers include all real numbers as well as imaginary numbers (real multiples of the imaginary unit i) and their sums.

Much of this course is focused on the sets $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Z}^+$. In fact, the study of number theory (seen in Topic 2) is exclusively concerned with integers.

The empty set and cardinality

Example. Write out the following sets explicitly.

- $A = \{x \in \mathbb{N} \mid x < 5\} = \{0, 1, 2, 3, 4\}$.
- $B = \{n \in \mathbb{Z} \mid n^2 = 4\} = \{-2, 2\}$.
- $C = \{x \in \mathbb{Z}^+ : \frac{x}{2} \in \mathbb{Z}\} = \{2, 4, 6, 8, \dots\}$.
- $D = \{2k : k \in \mathbb{Z}^+\} = \{2, 4, 6, 8, \dots\} = C$.
- $E = \{x \in D : x \notin \mathbb{R}\} = \{\}$.

Definition. The set with no elements is called the empty set, which is written as $\{\}$ or $\varnothing$.

Definition. The cardinality or size of a set is the number of distinct elements it contains. We write $|S|$ to mean "the cardinality of the set S". Note that if S is finite, then $|S| \in \mathbb{N}$.

Example. Find the cardinality of each of the sets from the previous example.

- $|A| = 5$.
- $|B| = 2$.
- $|C| = |D| = \infty$.
- $|E| = 0$.

Sets within sets

We have seen that sets can contain elements of any type. In particular, sets themselves can be contained in other sets. For example, if we think of tutorials as sets of students, then the set of all MATH1081 tutorials is a set containing sets.

For another example, consider the set $S = \{1, 2, \{3, 4\}\}$. It contains the elements 1, 2, and $\{3, 4\}$. This means we can write that $\{3, 4\} \in S$. This also tells us that the cardinality of S is given by $|S| = 3$. Notice that the elements of $\{3, 4\}$ are not related to the elements of S nor the cardinality of S. So in particular, in this case $3 \notin S$ and $4 \notin S$.

Example. Find the cardinality of each of the following sets.

- $|\{x, \{x\}\}| = 2$.
- $|\{x, y, \{x\}, \{y\}, \{x, y\}, \mathbb{N}\}| = 6$.
- $|\{x, \{x\}, \{x, x\}\}| = |\{x, \{x\}, \{x\}\}| = |\{x, \{x\}\}| = 2$.
- $|\{\{\}\}| = 1$.
- $|\{\{\{\}\}\}| = 1$.

Case study: Russell's paradox

Occasionally we will encounter "case studies", which are included to give more context to the topics we are studying.

These case studies are considered additional content and are not examinable.

In 1901, logician Bertrand Russell posed a problem that is now known as Russell's paradox (also attributed to Ernst Zermelo):

Problem. (Russell's paradox)
Let $S = \{\text{sets which are not elements of themselves}\}$. Is S an element of S?

- By the definition, any element $X \in S$ must satisfy $X \notin X$. Replacing X with S, we see that if $S \in S$, then $S \notin S$, which is a contradiction.
- Similarly, by the definition, any set such that $X \notin X$ must satisfy $X \in S$. Replacing X with S, we see that if $S \notin S$, then $S \in S$, which is again a contradiction.

So neither "$S \in S$" nor "$S \notin S$" can be true statements!

We mentioned earlier that a set must be well-defined. Russell's paradox provides an example of a set that is not well-defined, in this case due to its definition being self-referential.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 1 – Set theory and functions
Lecture 1.02 – Subsets and power sets

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Subsets

Note: The phrase "if and only if" is used in mathematical definitions to indicate equivalence of statements.

Definition. A set S is a subset of a set T if and only if every element of S is also an element of T.

Notation. We write $S \subseteq T$ to mean "S is a subset of T". Similarly, we write $S \not\subseteq T$ to indicate S is not a subset of T.

For example, we have $\{1,3\} \subseteq \{1,2,3\}$ and $\{1,2,3\} \subseteq \{1,2,3\}$, but $\{1,2,3,4\} \not\subseteq \{1,2,3\}$. We can also see that $\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Definition. Two sets S and T are equal (written $S = T$) if and only if they contain exactly the same elements. This means that every element of S is an element of T, and every element of T is an element of S. So we have that $S = T$ if and only if $S \subseteq T$ and $T \subseteq S$.

Definition. A set S is a proper subset of a set T if and only if $S \subseteq T$ and $S \neq T$. (Equivalently, $S \subseteq T$ and $T \not\subseteq S$.)

Notation. We write $S \subset T$ or $S \subsetneq T$ to mean "S is a proper subset of T".

For example, we have $\{1,3\} \subset \{1,2,3\}$, but $\{1,2,3\} \not\subset \{1,2,3\}$.

Example – Identifying elements and subsets

Example. Decide whether each of the statements below is true or false.

- $1 \in \{1, \{1\}\}$ is a true statement since 1 is an element of $\{1, \{1\}\}$.
- $1 \subseteq \{1, \{1\}\}$ is a false statement since 1 is not a set, so it cannot be a subset.
- $\{1\} \in \{1, \{1\}\}$ is a true statement since $\{1\}$ is an element of $\{1, \{1\}\}$.
- $\{1\} \subseteq \{1, \{1\}\}$ is a true statement since every element of $\{1\}$ is an element of $\{1, \{1\}\}$.
- $\{\{1\}\} \in \{1, \{1\}\}$ is a false statement since $\{\{1\}\}$ is not an element of $\{1, \{1\}\}$.
- $\{\{1\}\} \subseteq \{1, \{1\}\}$ is a true statement since every element of $\{\{1\}\}$ is an element of $\{1, \{1\}\}$.

Theorem. For any set S, we have $S \subseteq S$ and $\{\} \subseteq S$.

Proof. Clearly $S \subseteq S$, since every element of S is again an element of S. The statement $\{\} \subseteq S$ is vacuously true since every element of $\{\}$ (of which there are none) is an element of S.

Proving statements about set containment

Suppose that S and T are sets. To prove that S is a subset of T, we must show that every element of S is also an element of T. If S is very large, it might be impractical to check each element of S individually. So we typically prove that any arbitrary element of S also belongs to T by working with a general element $x \in S$.

That is, to prove that $S \subseteq T$, we write a proof with the following structure:

Let $x \in S$ be an arbitrary element of S.
$\vdots$
Then $x \in T$.
Thus $S \subseteq T$.

To prove that $S \not\subseteq T$, we only have to show that there is some particular element in S that is not in T. Such a proof would have the structure:

Choose $x \in S$ to be the particular element...
$\vdots$
Then $x \notin T$.
Thus $S \not\subseteq T$.

Example – Proving set containment

Example. Let $S = \{2k+1 \ : \ k \in \mathbb{Z}\}$ and $T = \{4n-1 \ : \ n \in \mathbb{Z}\}$. Prove that $S \not\subseteq T$.

Solution. Consider the number 1. Clearly $1 \in S$, since $1 = 2 \times 0 + 1$ and $0 \in \mathbb{Z}$. However $1 \notin T$, since the only solution to $1 = 4n - 1$ is $n = \frac{1}{2}$, which is not an integer. Thus 1 is an element of S that is not an element of T, meaning that $S \not\subseteq T$.

Example. Let $S = \{6k+1 \ : \ k \in \mathbb{Z}\}$ and $T = \{3n-2 \ : \ n \in \mathbb{Z}\}$. Prove that $S \subseteq T$.

Solution. Let $x \in S$ be an arbitrary element of S. Then $x = 6k + 1$ for some integer k. We can rewrite this as

$$x = 6k + 1 = 3(2k + 1) - 2,$$

so $x = 3n - 2$ where $n = 2k + 1$ is some integer. This means that $x \in T$, so any element of S is also an element of T, and thus $S \subseteq T$.

Proving further statements about set containment

To prove that $S = T$, we must prove that $S \subseteq T$ and that $T \subseteq S$. Note that this means we must provide two separate proofs (using the structure shown on the previous slide).

To prove that $S \neq T$, we must prove that $S \not\subseteq T$ or that $T \not\subseteq S$. Note that this just means we have to show there is some particular element that belongs to one of the sets but not the other.

To prove that $S \subset T$, we must prove that $S \subseteq T$ and that $S \neq T$. Note that this means after proving that $S \subseteq T$, we just have to find some particular element of T that is not in S.

(To prove that $S \not\subset T$, we must prove that $S \not\subseteq T$ or that $S = T$.)

Example. Let $S = \{6k + 1 \ : \ k \in \mathbb{Z}\}$ and $T = \{3n - 2 \ : \ n \in \mathbb{Z}\}$.
We have already shown that $S \subseteq T$. Prove that S is a proper subset of T.

Solution. To prove that $S \subset T$, it remains to show that $S \neq T$.

Consider the number 4. Clearly $4 \in T$, since $4 = 3 \times 2 - 2$ and $2 \in \mathbb{Z}$. However $4 \notin S$, since the only solution to $4 = 6k + 1$ is $k = \frac{1}{2}$, which is not an integer. Thus 4 is an element of T that is not an element of S, meaning that $S \neq T$. Since we already know $S \subseteq T$, we can conclude that $S \subset T$.

Example – Proving set equality

Example. Let $S = \{6k+1 \ : \ k \in \mathbb{Z}\}$ and $T = \{6n-5 \ : \ n \in \mathbb{Z}\}$. Prove that $S = T$.

Solution. We need to prove both that $S \subseteq T$ and that $T \subseteq S$.

Proving $S \subseteq T$: Let $x \in S$ be an arbitrary element of S. Then $x = 6k+1$ for some integer k. We can rewrite this as

$$x = 6k + 1 = 6(k+1) - 5,$$

so $x = 6n - 5$ where $n = k + 1$ is some integer. This means that $x \in T$, so any element of S is also an element of T, and thus $S \subseteq T$.

Proving $T \subseteq S$: Let $x \in T$ be an arbitrary element of T. Then $x = 6n-5$ for some integer n. We can rewrite this as

$$x = 6n - 5 = 6(n-1) + 1,$$

so $x = 6k + 1$ where $k = n - 1$ is some integer. This means that $x \in S$, so any element of T is also an element of S, and thus $T \subseteq S$.

Since we have now shown that both $S \subseteq T$ and $T \subseteq S$, we can conclude that $S = T$.

Power sets

Definition. The power set of a set S, written as $\mathcal{P}(S)$ or just $P(S)$, is the set of all possible subsets of S.

For example, the subsets of $\{1, 2\}$ are $\{\}$, $\{1\}$, $\{2\}$, and $\{1, 2\}$, so the power set of $\{1, 2\}$ is $\mathcal{P}(\{1, 2\}) = \{\, \{\}, \{1\}, \{2\}, \{1, 2\} \,\}$.

Example. Find $\mathcal{P}(\{a, b, c\})$.

Solution. We first list the subsets of $\{a, b, c\}$ in increasing size order:

- The only subset of size 0 is $\{\}$.
- The subsets of size 1 are $\{a\}$, $\{b\}$, and $\{c\}$.
- The subsets of size 2 are $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$.
- The only subset of size 3 is $\{a, b, c\}$.

Thus $\mathcal{P}(\{a, b, c\}) = \{\, \{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\} \,\}$.

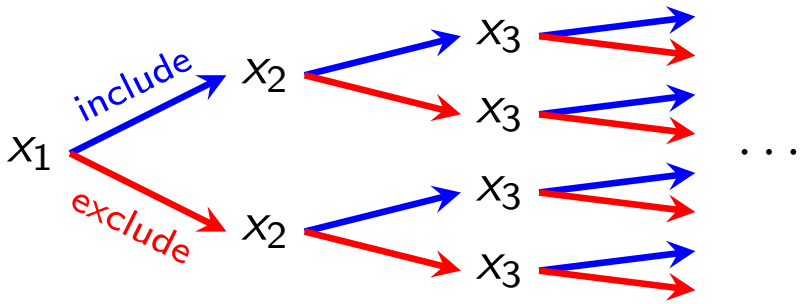
Notice that $|\mathcal{P}(\{1, 2\})| = 4 = 2^2$, while $|\mathcal{P}(\{a, b, c\})| = 8 = 2^3$. We can also easily check that $|\mathcal{P}(\{1\})| = 2^1$ and $|\mathcal{P}(\{\})| = 2^0$. This seems to indicate a connection between cardinalities of power sets and powers of 2...

Cardinality of power sets

Theorem. For any finite set S, the cardinality of its power set is given by

$$|\mathcal{P}(S)| = 2^{|S|}.$$

Proof. Since S is finite, we may write $S = \{x_1, x_2, x_3, \ldots, x_n\}$ where $n = |S|$ and each x_i is a different element of S. We can think of creating a subset of S by choosing for each element whether it is included or excluded in the subset. These branching choices can be represented by the tree diagram:



Each path from left to right produces a different subset of S, and all possible subsets are accounted for. At each step, the number of branches doubles, and the last choice is for x_n at the nth step. So there are $2^n = 2^{|S|}$ total different paths available, and thus there are $2^{|S|}$ different subsets of S.

Example. Find the following cardinalities:

- $|\mathcal{P}(\{1,2,3,4\})| = 2^4 = 16.$
- $|\mathcal{P}(\mathcal{P}(\{1\}))| = 2^{|\mathcal{P}(\{1\})|} = 2^{2^1} = 4.$

Proofs involving power sets

The following fact follows straight from our definition of a power set, and can be useful when proving properties of power sets.

Fact. For any sets S and T, we have $S \subseteq T$ if and only if $S \in \mathcal{P}(T)$.

In order to prove a statement involving power sets, we first introduce a lemma about sets. ("Lemma" in mathematics means a minor theorem.)

Lemma. Suppose A, B, and C are sets such that $A \subseteq B$ and $B \subseteq C$. Then $A \subseteq C$.

Proof. Try this yourself! (See tutorial Problem Set 1, Question 7.)

Example. Suppose that S and T are sets such that $S \subseteq T$. Prove that $\mathcal{P}(S) \subseteq \mathcal{P}(T)$.

Solution. Let $X \in \mathcal{P}(S)$ be an arbitrary element of $\mathcal{P}(S)$. Then $X \subseteq S$ by the definition of a power set. Since $S \subseteq T$, by the above lemma we know that $X \subseteq T$. This means that $X \in \mathcal{P}(T)$, so any element of $\mathcal{P}(S)$ is also an element of $\mathcal{P}(T)$, and thus $\mathcal{P}(S) \subseteq \mathcal{P}(T)$.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 1 – Set theory and functions
Lecture 1.03 – Venn diagrams and set operations

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

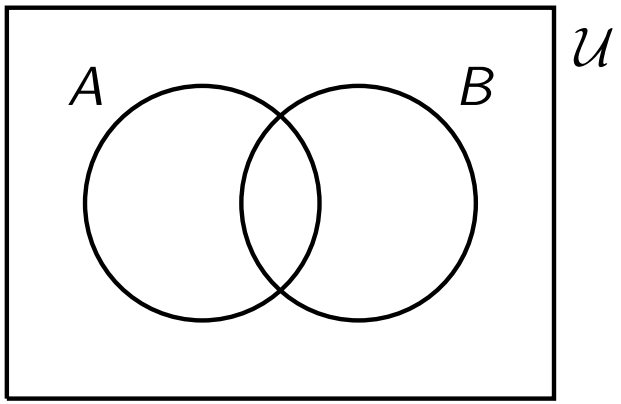
Venn diagrams

Definition. When working with related sets, it can be useful to define a universal set which contains all elements relevant to these sets. The universal set is usually denoted by $\mathcal{U}$ or just U. In particular, all the related sets are subsets of $\mathcal{U}$.

For example, if our sets are MATH1081 tutorials, then an appropriate universal set might be the set of all MATH1081 students. If our sets are intervals on the real number line, then the universal set would be $\mathbb{R}$.

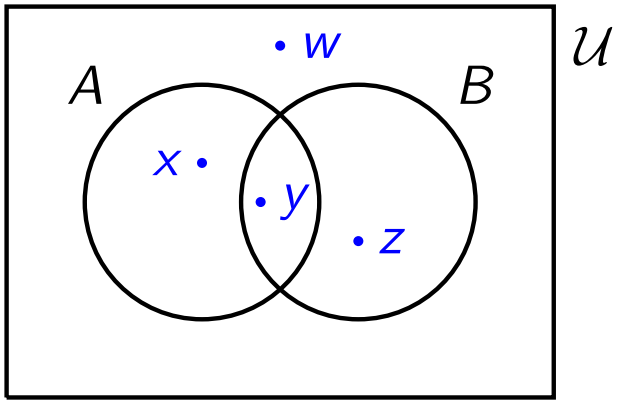
Definition. A Venn diagram is a diagrammatic tool for visualising relationships between related sets. Sets are represented as overlapping closed figures (usually circles) within a larger figure (usually a rectangle) representing the universal set. Elements can be represented as points placed within different sections of the diagram to show which sets they belong to.

For example, here is a general Venn diagram for two sets A and B with universal set $\mathcal{U}$:



Venn diagram example

Example. Consider the following Venn diagram:



For each of the elements $w, x, y, z \in \mathcal{U}$, we can make the following conclusions:

- $w \notin A$ and $w \notin B$.
- $x \in A$ and $x \notin B$.
- $y \in A$ and $y \in B$.
- $z \notin A$ and $z \in B$.

In order to more easily refer to the different sections in a Venn diagram, we shall introduce new notation that allows us to perform operations on sets.

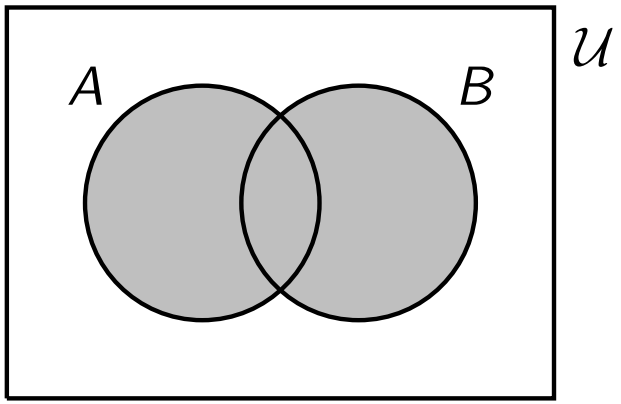
Union

Definition. The union of two sets A and B, written as $A \cup B$, is the set of all elements in A or B (or both). That is,

$$A \cup B = \{x \in \mathcal{U} \ : \ x \in A \ \text{ or } \ x \in B\}.$$

(Note: The word "or" in mathematics is always treated as inclusive.)

In a Venn diagram, $A \cup B$ is represented by this shaded region:



Example. Given that $R = \{a, c, e\}$, $S = \{b, d\}$, and $T = \{d, e, f\}$, find the following:

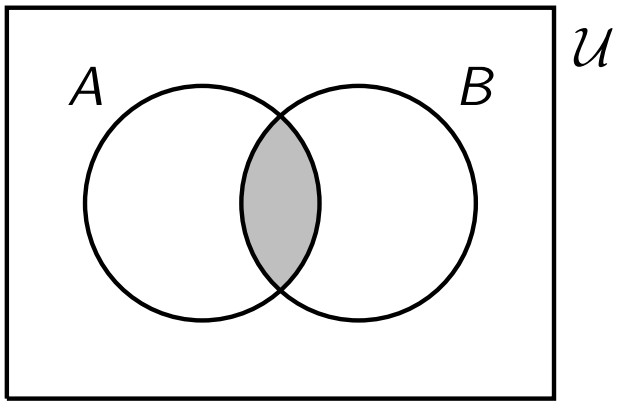
- $R \cup S = \{a, b, c, d, e\}$.
- $R \cup T = \{a, c, d, e, f\}$.
- $S \cup T = \{b, d, e, f\}$.
- $R \cup S \cup T = \{a, b, c, d, e, f\}$.

Intersection

Definition. The intersection of two sets A and B, written as $A \cap B$, is the set of all elements in both A and B. That is,

$$A \cap B = \{x \in \mathcal{U} \ : \ x \in A \ \text{ and } \ x \in B\}.$$

In a Venn diagram, $A \cap B$ is represented by this shaded region:



Example. Given that $R = \{a, c, e\}$, $S = \{b, c, d\}$, and $T = \{a, b, d, e\}$, find the following:

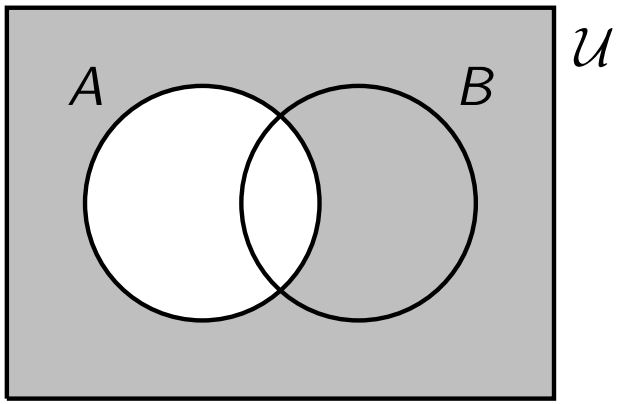
- $R \cap S = \{c\}$.
- $R \cap T = \{a, e\}$.
- $S \cap T = \{b, d\}$.
- $R \cap S \cap T = \{\}$.

Complement

Definition. The complement of a set A, written as A^c (or sometimes $\overline{A}$), is the set of all elements in the universal set that are not in A. That is,

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

In a Venn diagram, A^c is represented by this shaded region:



Example. Given that $\mathcal{U} = \{a, b, c, d, e\}$, $R = \{a, c, e\}$, $S = \{b\}$, and $T = \{\}$, find the following:

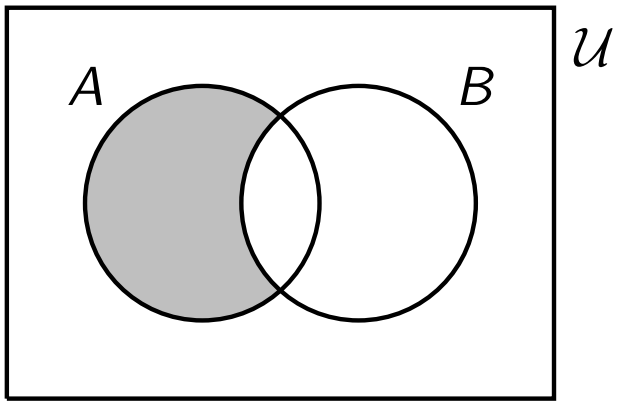
- $R^c = \{b, d\}$.
- $S^c = \{a, c, d, e\}$.
- $T^c = \{a, b, c, d, e\}$.

Set difference

Definition. The difference of two sets A and B, written as $A - B$ (or sometimes $A \setminus B$), is the set of all elements in A which are not in B. That is,

$$A - B = \{x \in \mathcal{U} \ : \ x \in A \ \text{ and } \ x \notin B\}.$$

In a Venn diagram, $A - B$ is represented by this shaded region:



Example. Given that $R = \{a, b, c, d\}$, $S = \{b, c, d\}$, and $T = \{b, d, e\}$, find the following:

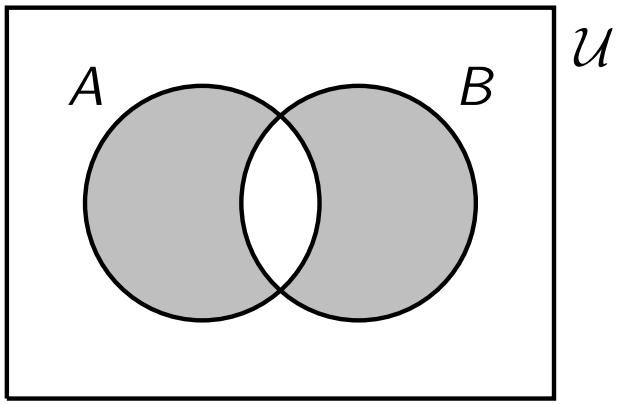
- $R - S = \{a\}$.
- $R - T = \{a, c\}$.
- $S - T = \{c\}$.
- $S - R = \{\}$. (Notice that in general, $A - B \neq B - A$ for sets A and B.)

Symmetric difference

Definition. The symmetric difference of two sets A and B, written as $A \ominus B$ (or sometimes $A \triangle B$ or $A \oplus B$), is the set of all elements in A or B, but not both. That is,

$$A \ominus B = \{x \in \mathcal{U} \ : \ x \in A \cup B \ \text{ and } \ x \notin A \cap B\}.$$

In a Venn diagram, $A \ominus B$ is represented by this shaded region:

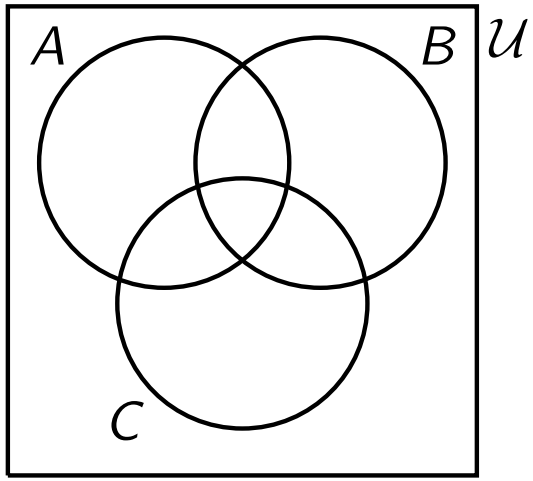


Example. Given that $R = \{a, b, c\}$, $S = \{b\}$, and $T = \{b, c, d\}$, find the following:

- $R \ominus S = \{a, c\}$.
- $R \ominus T = \{a, d\}$.
- $S \ominus T = \{c, d\}$.

Combining set operations

A general Venn diagram for three sets A, B, and C with universal set $\mathcal{U}$ is shown to the right.

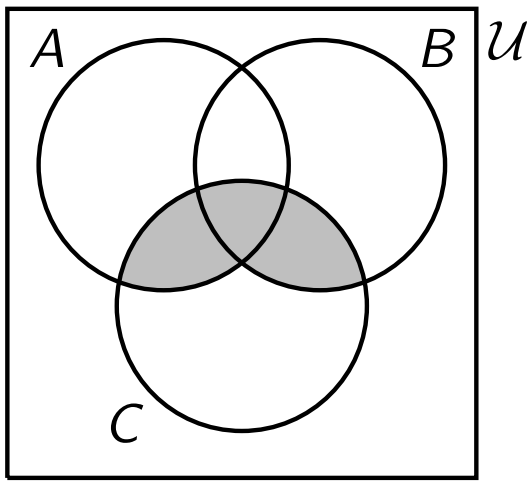


Venn diagrams for four or more sets can become unwieldy or impossible to draw, so they are normally avoided.

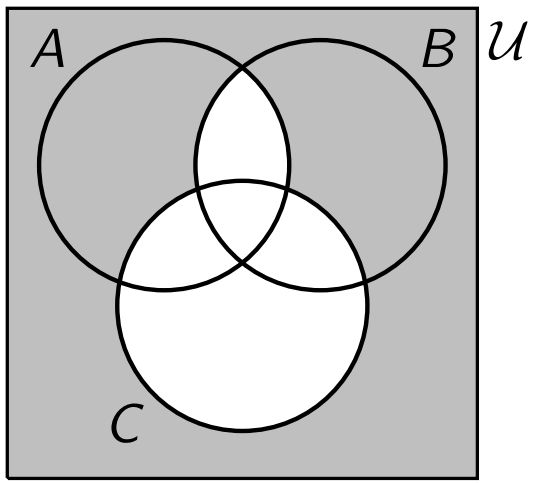
Set operations can be applied to multiple sets, so long as the order of operations is clearly indicated by the use of brackets.

Example. Shade the regions indicated by the following set expressions.

$(A \cup B) \cap C$



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



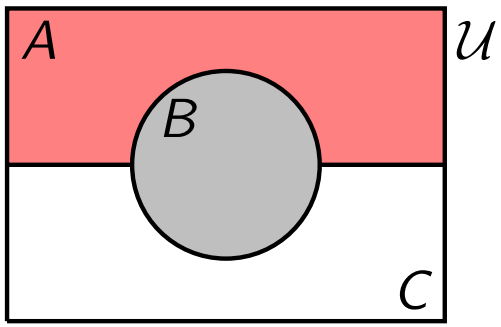
Disjoint sets

Definition. Two sets A and B are disjoint if their intersection is empty, that is, if $A \cap B = \varnothing$.

Definition. The sets $A_1, A_2, A_3, \ldots, A_k$ are pairwise disjoint if every pair of sets is disjoint, that is, if $A_i \cap A_j = \varnothing$ for all $i \neq j$.

Definition. The sets $A_1, A_2, A_3, \ldots, A_k$ partition the set B if they are pairwise disjoint and $A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_k = B$.

For example, in the Venn diagram on the right, $\mathcal{U}$ is partitioned by the sets A, B, and C.



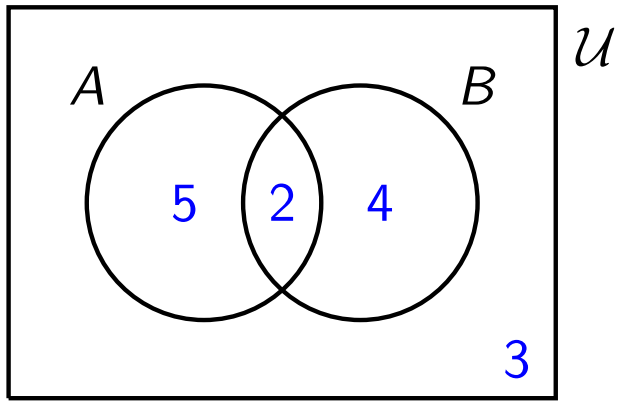
Example. Complete the following sentences regarding general sets A and B:

- A and A^c partition $\mathcal{U}$.
- A and $B - A$ partition $A \cup B$.
- $A \cap B$ and $A \ominus B$ partition $A \cup B$.
- $A \cap B$ and $A - B$ partition A.

Cardinalities in Venn diagrams

Another way to represent information in a Venn diagram is by writing the cardinality of each individual section in the diagram. Cardinalities can be represented as numbers placed within each section (without points, to distinguish set cardinalities from set elements).

Example. Consider the following Venn diagram:



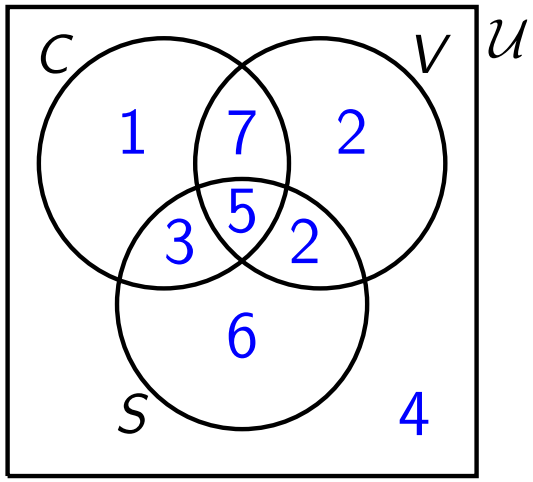
Find each of the following:

- $|A \cap B| = 2$.
- $|A| = 7$.
- $|A \cup B| = 11$.
- $|\mathcal{U}| = 14$.

Example – Finding cardinalities with a Venn diagram

Example. 30 people were asked to select their preferred ice-cream flavours from a list, where more than one selection was allowed. 16 people selected chocolate, 16 selected vanilla, and 16 selected strawberry. 12 people selected both chocolate and vanilla, 8 people selected both chocolate and strawberry, and 7 people selected both vanilla and strawberry. 5 people selected all three flavours. How many surveyed people selected none of the three flavours?

Solution. Let C, V, and S be the set of people who selected chocolate, vanilla, and strawberry respectively. Drawing up a Venn diagram, we can fill out the cardinalities by working from the innermost section outwards:



So the answer is 4.

Inclusion-exclusion principle

Theorem. (Inclusion-exclusion principle)
The cardinality of a union of sets can be expressed in terms of cardinalities of their intersections. For example,

- For any two sets A and B, we have

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

- For any three sets A, B, and C, we have

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|.$$

Proof (sketch). In the case of two sets, finding $|A| + |B|$ counts each element of $A \cup B$ at least once, but elements that belong to both A and B are counted twice. To account for this, we subtract the size of $A \cap B$. The cases for three or more sets work similarly.

Example. Solve the previous problem using the inclusion-exclusion principle.

Solution. Using the inclusion-exclusion principle, we have

$$\begin{aligned} |C \cup V \cup S| &= |C| + |V| + |S| - |C \cap V| - |C \cap S| - |V \cap S| + |C \cap V \cap S| \\ &= 16 + 16 + 16 - 12 - 8 - 7 + 5 = 26, \end{aligned}$$

so the number of people who chose none of the flavours is $30 - 26 = 4$.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 1 – Set theory and functions
Lecture 1.04 – Laws of set algebra

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Proofs involving set operations

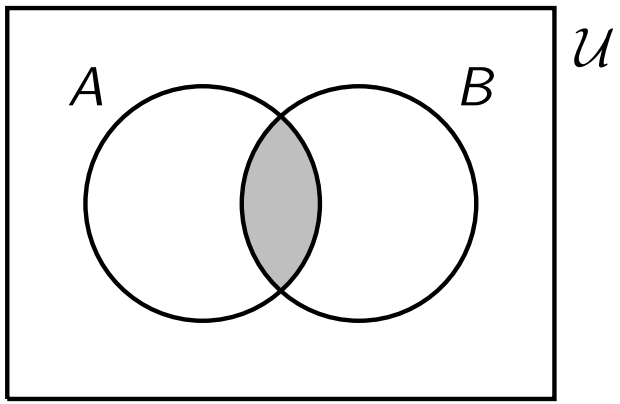
There are three main ways to justify or prove a statement involving set operations:

- Using Venn diagrams.
  - Venn diagrams are a useful visual aide, but are not generally considered valid tools for rigorous proofs.
- Using set operation definitions, and thinking in terms of arbitrary elements.
  - This method is reliable and a good tool for most proofs. Using this method to prove equivalence of sets can sometimes become unwieldy, since two containment proofs are required.
- Using the laws of set algebra.
  - We will soon introduce the laws of set algebra, which are especially helpful in simplifying expressions.

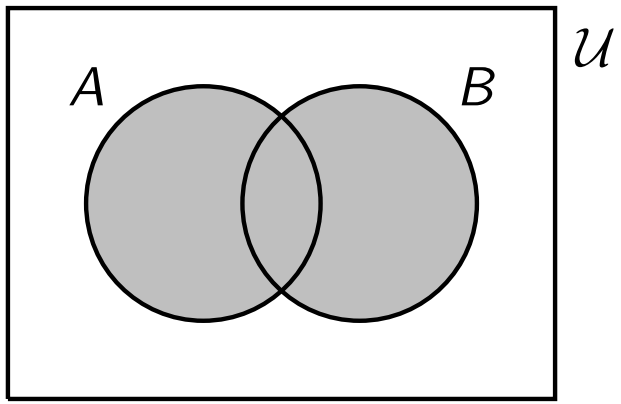
Example 1

Example. Is $A \cap B$ a subset of $A \cup B$ for all sets A and B?

Working: Considering the Venn diagrams for both sets, we have:



$A \cap B$



$A \cup B$

Since the shaded region on the left is completely contained within the shaded region on the right, this indicates that it is true in general that $A \cap B \subseteq A \cup B$.

Proof. Let $x \in A \cap B$ be an arbitrary element of $A \cap B$. Then $x \in A$ and $x \in B$. Since $x \in A$, we can certainly say $x \in A$ or $x \in B$. So $x \in A \cup B$. Thus since any element of $A \cap B$ is an element of $A \cup B$, we have that $A \cap B \subseteq A \cup B$.

Example 2

Example. Prove that for any sets A and B, we have $A - B = A \cap B^c$.

Proof. We need to show both that $A - B \subseteq A \cap B^c$, and that $A \cap B^c \subseteq A - B$.

First, let $x \in A - B$. Then $x \in A$ and $x \notin B$. So $x \in A$ and $x \in B^c$. Thus $x \in A \cap B^c$, meaning that $A - B \subseteq A \cap B^c$.

Next, let $x \in A \cap B^c$. Then $x \in A$ and $x \in B^c$. So $x \in A$ and $x \notin B$. Thus $x \in A - B$, meaning that $A \cap B^c \subseteq A - B$.

Hence since the sets are subsets of each other, we know $A - B = A \cap B^c$.

Alternative proof. We have

$$\begin{aligned} A - B &= \{x \in \mathcal{U} \ : \ x \in A \ \text{ and } \ x \notin B\} \\ &= \{x \in \mathcal{U} \ : \ x \in A \ \text{ and } \ x \in B^c\} \\ &= A \cap B^c, \end{aligned}$$

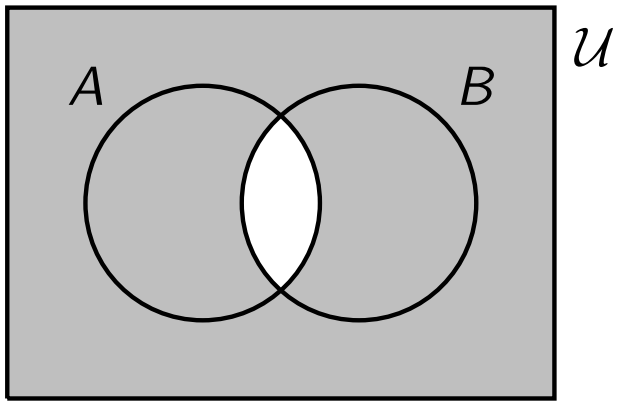
as required.

Note that this second style of proof is more efficient, but may not always be applicable depending on the problem.

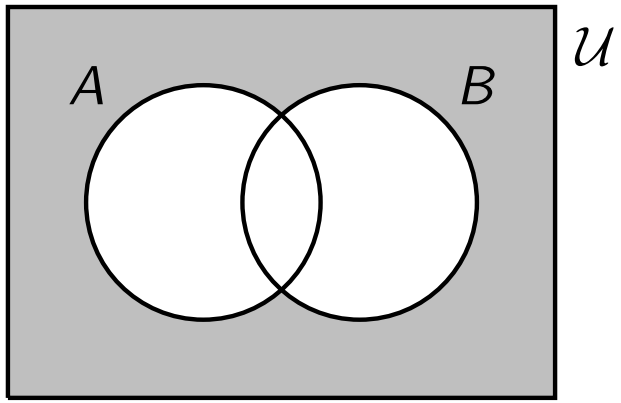
Example 3

Example. Are the sets $(A \cap B)^c$ and $A^c \cap B^c$ equal for all sets A and B?

Working: Considering the Venn diagrams for both sets, we have:



$(A \cap B)^c$



$A^c \cap B^c$

Since the shaded regions on the left and right are not identical, this indicates that in general $(A \cap B)^c \neq A^c \cap B^c$. To prove this, we just need to provide an example where a non-matching section contains at least one element.

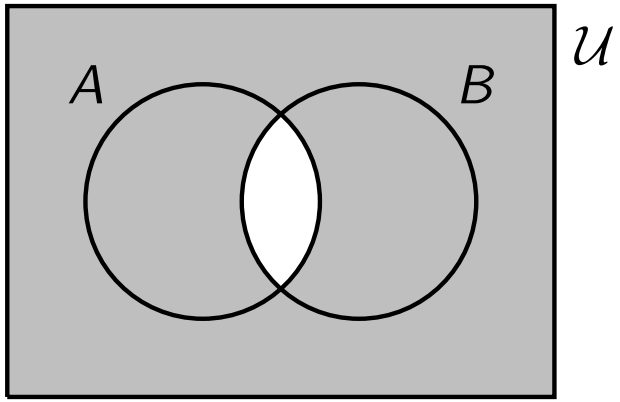
Proof. Consider the case where $A = \{1\}$ and $B = \{2\}$, with universal set $\mathcal{U} = \{1, 2, 3\}$. Then we have $(A \cap B)^c = (\{\})^c = \{1, 2, 3\}$, while $A^c \cap B^c = \{2, 3\} \cap \{1, 3\} = \{3\}$. Since these two sets are not the same, we know $(A \cap B)^c \neq A^c \cap B^c$ in general.

Note that this is one of many valid cases that demonstrate inequality. An even simpler case is $A = \{1\}$, $B = \{\}$, and $\mathcal{U} = \{1\}$.

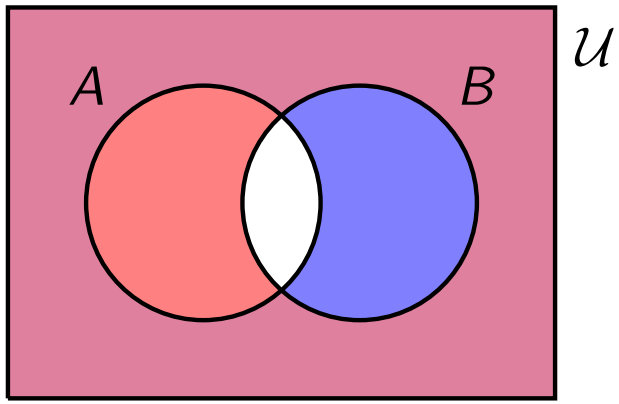
Example 4

Example. Are the sets $(A \cap B)^c$ and $A^c \cup B^c$ equal for all sets A and B?

Working: Considering the Venn diagrams for both sets, we have:



$(A \cap B)^c$



$A^c \cup B^c$

Since the shaded regions on the left and right are identical, this indicates that it is true in general that $(A \cap B)^c = A^c \cup B^c$.

Example 4 (continued)

Example. Are the sets $(A \cap B)^c$ and $A^c \cup B^c$ equal for all sets A and B?

Proof. We claim that the sets are equal, so we want to show both that $A^c \cup B^c \subseteq (A \cap B)^c$, and that $(A \cap B)^c \subseteq A^c \cup B^c$.

First, let $x \in A^c \cup B^c$. Then $x \in A^c$ or $x \in B^c$, so we can say $x \notin A$ or $x \notin B$. So x certainly can't be an element of both A and B at once, meaning $x \notin A \cap B$. So $x \in (A \cap B)^c$, and thus $A^c \cup B^c \subseteq (A \cap B)^c$.

Next, let $x \in (A \cap B)^c$. Then $x \notin A \cap B$. Either $x \in A$ or $x \notin A$, so we consider these two cases in turn.

Case 1: If $x \in A$, then since $x \notin A \cap B$, we must have that $x \notin B$. So $x \in B^c$, meaning that $x \in A^c \cup B^c$.

Case 2: If $x \notin A$, then $x \in A^c$, meaning that $x \in A^c \cup B^c$.

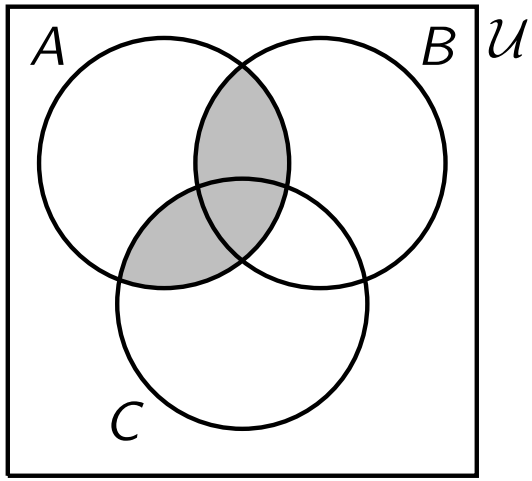
Since $x \in A^c \cup B^c$ in both cases, we can conclude that $(A \cap B)^c \subseteq A^c \cup B^c$.

Hence since the sets are subsets of each other, we can conclude that $(A \cap B)^c = A^c \cup B^c$.

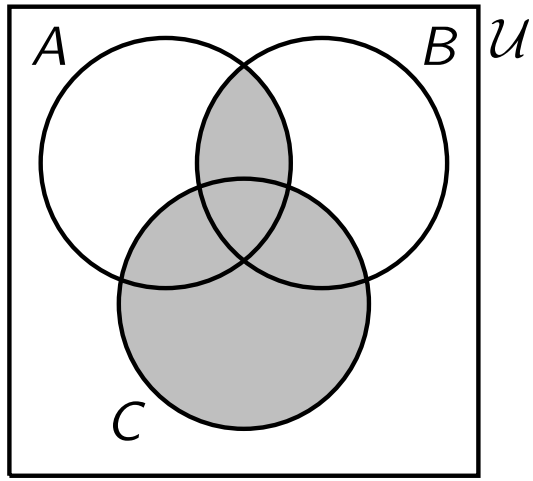
Example 5

Example. Are $A \cap (B \cup C)$ and $(A \cap B) \cup C$ equal for all sets A, B, and C?

Working: Considering the Venn diagrams for both sets, we have:



$A \cap (B \cup C)$



$(A \cap B) \cup C$

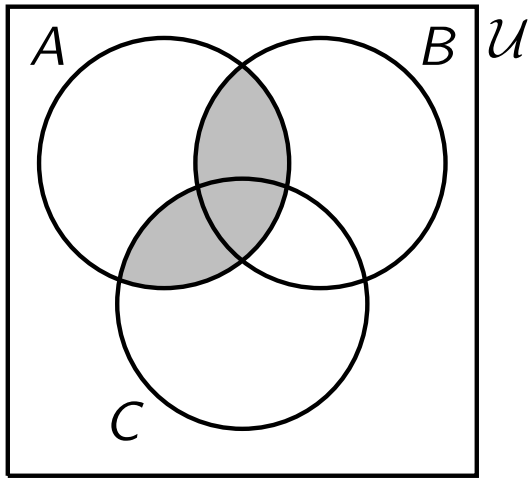
Since the shaded regions on the left and right are not identical, this indicates that in general $A \cap (B \cup C) \neq (A \cap B) \cup C$. To prove this, we just need to provide an example where a non-matching section contains an element.

Proof. Consider the case where $A = B = \{\}$ and $C = \{1\}$. Then we have $A \cap (B \cup C) = \{\} \cap \{1\} = \{\}$, while $(A \cap B) \cup C = \{\} \cup \{1\} = \{1\}$. Since these two sets are not the same, we conclude $A \cap (B \cup C) \neq (A \cap B) \cup C$ in general.

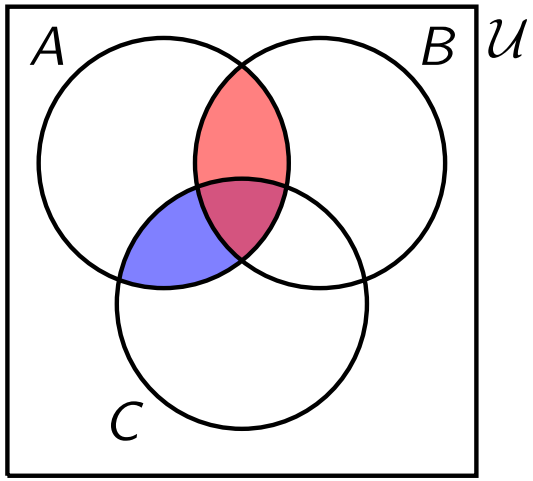
Example 6

Example. Are $A \cap (B \cup C)$ and $(A \cap B) \cup (A \cap C)$ equal for all sets A, B, C?

Working: Considering the Venn diagrams for both sets, we have:



$A \cap (B \cup C)$



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

Since the shaded regions on the left and right are identical, this indicates that it is true in general that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. Try this yourself! (Use similar methods to Examples 2 and 4.)

Laws of set algebra

For any sets A, B, C with universal set $\mathcal{U}$ and empty set $\varnothing$, we have the following laws of set algebra:

Commutativity:

$$A \cup B = B \cup A,$$
$$A \cap B = B \cap A.$$

Associativity:

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

Distributivity:

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

Absorption:

$$A \cup (A \cap B) = A,$$
$$A \cap (A \cup B) = A.$$

Idempotence:

$$A \cup A = A,$$
$$A \cap A = A.$$

Identity:

$$A \cup \varnothing = A,$$
$$A \cap \mathcal{U} = A.$$

Domination:

$$A \cup \mathcal{U} = \mathcal{U},$$
$$A \cap \varnothing = \varnothing.$$

Complement law:

$$A \cup A^c = \mathcal{U},$$
$$A \cap A^c = \varnothing.$$

Double complement law:

$$(A^c)^c = A.$$

De Morgan's law:

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

We also have the following definitions:

Difference:

$$A - B = A \cap B^c.$$

Symmetric difference:

$$A \ominus B = (A \cup B) - (A \cap B).$$

Comments on the laws of set algebra

The laws of set algebra completely describe the behaviour of sets under the basic set operations. It is possible to verify any statements involving set expressions by using only these laws, though doing so can take a lot of work.

While there are many laws to learn here, almost all of them are easily justified by considering them in terms of Venn diagrams.

When simplifying expressions or proving statements using the laws of set algebra, we should always state which laws are being used at each step. If you do not remember the name of a particular law, you may instead describe it in words and/or provide its general definition.

Definition. The dual of a set expression is the expression obtained by replacing every instance of $\cup$ with $\cap$, $\cap$ with $\cup$, $\varnothing$ with $\mathcal{U}$, and $\mathcal{U}$ with $\varnothing$.

Theorem. (Duality principle)
Any statement involving only sets and the union, intersection, and complement operations is true if and only if its dual statement is true.

Proof. This is a consequence of the fact that every law of set algebra consists of a pair of dual statements (except for the double complement law, which is self-dual).

Example – Simplifying set expressions

Example. Simplify the set expression $A \cap (A \cap B^c)^c$.

Solution. We proceed using the laws of set algebra:

$$\begin{aligned}
A \cap (A \cap B^c)^c &= A \cap (A^c \cup (B^c)^c) && \text{(De Morgan's law)} \\
&= A \cap (A^c \cup B) && \text{(double complement law)} \\
&= (A \cap A^c) \cup (A \cap B) && \text{(distributivity)} \\
&= \varnothing \cup (A \cap B) && \text{(complement law)} \\
&= (A \cap B) \cup \varnothing && \text{(commutativity)} \\
&= A \cap B && \text{(identity).}
\end{aligned}$$

Notice that some of these steps could have been performed at the same time, for example the commutativity and identity applications.

We could also have checked this by using a Venn diagram, though remember that a Venn diagram explanation would not constitute a rigorous proof.

The dual of this result must also be true, so we now also know that: $A \cup (A \cup B^c)^c = A \cup B$.

Example – Proving equivalence of set expressions

Example. Show that $(A - B) \cap (A - C) = A - (B \cup C)$ for all sets A, B, C.

Solution. We proceed using the laws of set algebra. Simplifying the left-hand side yields:

$$\begin{aligned}
(A - B) \cap (A - C) &= (A \cap B^c) \cap (A \cap C^c) && \text{(def'n of difference)} \\
&= A \cap (B^c \cap A) \cap C^c && \text{(associativity)} \\
&= A \cap (A \cap B^c) \cap C^c && \text{(commutativity)} \\
&= (A \cap A) \cap B^c \cap C^c && \text{(associativity)} \\
&= A \cap B^c \cap C^c && \text{(idempotence).}
\end{aligned}$$

Simplifying the right-hand side yields:

$$\begin{aligned}
A - (B \cup C) &= A \cap (B \cup C)^c && \text{(def'n of difference)} \\
&= A \cap (B^c \cap C^c) && \text{(De Morgan's law)} \\
&= A \cap B^c \cap C^c && \text{(associativity).}
\end{aligned}$$

Since both expressions simplify to give the same set, they must be equal. So we have shown that $(A - B) \cap (A - C) = A - (B \cup C)$.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 1 – Set theory and functions
Lecture 1.05 – Cartesian product and functions

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Cartesian product

Definition. A tuple is a finite, ordered collection of objects. Unlike for a set, the order of the elements in a tuple is important, and elements may be repeated. A tuple with exactly n elements is sometimes called an n-tuple. A tuple with exactly 2 elements is also called an ordered pair.

Notation. A tuple can be represented by writing its elements surrounded by parentheses. For example, $(1, 2, 1)$ is a 3-tuple, and it is different to $(1, 1, 2)$.

Definition. The Cartesian product of two sets A and B, denoted $A \times B$, is the set containing all ordered pairs (2-tuples) for which the first element is an element of A, and the second element is an element of B. That is,

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

Notation. We sometimes refer to the Cartesian product $A \times A$ as A^2. For example, the real coordinate plane is often referred to as $\mathbb{R}^2$.

Example. Suppose $A = \{1, 2\}$ and $B = \{x, y, z\}$. Evaluate the following.

- $A \times B = \{ (1, x), (1, y), (1, z), (2, x), (2, y), (2, z) \}$.
- $A^2 = \{ (1, 1), (1, 2), (2, 1), (2, 2) \}$.

Fact. For any sets A and B, we have $|A \times B| = |A| \times |B|$.

Functions

We typically think of a function as a rule that converts input values to output values. To properly define what this means, we will use the language of set theory.

Definition. Given sets X and Y, a function from X to Y is a subset of $X \times Y$ which contains exactly one ordered pair (x, y) for each $x \in X$.

Notation. A function f from a set X to a set Y is declared as $f : X \to Y$. If $(x, y) \in f$, we can say "f maps x to y". Instead of writing $(x, y) \in f$, we can also write $f : x \mapsto y$, or (more commonly) $f(x) = y$. We sometimes refer to x as an input value of f, and y as the output value of x under f.

For example, if $X = \{a, b, c\}$ and $Y = \{1, 2\}$, then a valid function $f : X \to Y$ is given by $f = \{(a, 1), (b, 2), (c, 2)\}$. This means we can write that $f(a) = 1$, $f(b) = 2$, and $f(c) = 2$.

We can also define a function using a formula. For example, consider the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ for all $x \in \mathbb{R}$. This function when interpreted as a subset of $\mathbb{R}^2$ has infinitely many elements, including $(1, 1)$, $(2, 4)$, $(-2, 4)$, and $(\sqrt{2}, 2)$.

Example – Identifying functions

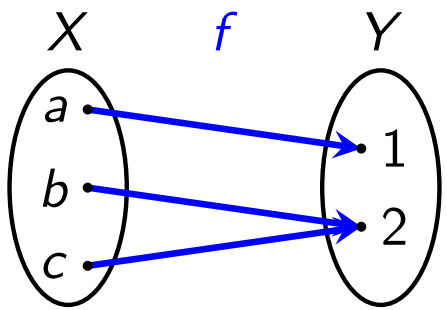
Example. Suppose $X = \{1, 2, 3\}$ and $Y = \{a, b, c, d\}$. Which of the following represent functions from X to Y?

- $\{(1, a), (2, b), (3, a)\}$ is a function, since there is exactly one output value for each possible input value. The fact that c and d are never returned as output values has no effect on whether f is a function.
- $\{(1, a), (2, b), (3, c), (d, 1)\}$ is not a function, since it includes the element $(d, 1)$, but $d \notin X$ is not a valid possible input and $1 \notin Y$ is not a valid possible output.
- $\{(1, a), (2, b)\}$ is not a function, since it does not define an output for the input value $3 \in X$; that is, it does not include the element $(3, y)$ for any $y \in Y$.
- $\{(1, a), (2, b), (3, c), (3, d)\}$ is not a function, since it defines more than one output for the input value $3 \in X$; that is, it includes the elements $(3, c)$ and $(3, d)$ where the first element is the same but the second element is different.

Arrow diagrams

It can sometimes be useful to represent a function $f : X \to Y$ visually. One way this can be done is by using arrow diagrams. Just like for Venn diagrams, the sets X and Y are represented as separate closed figures, and their elements are represented as labelled points. The function is then represented by a series of arrows, each pointing from an input value in X to its corresponding output value in Y.

For example, in the case with sets $X = \{a, b, c\}$ and $Y = \{1, 2\}$, and function $f : X \to Y$ given by $f = \{(a, 1), (b, 2), (c, 2)\}$, the function f can be represented with an arrow diagram as follows:

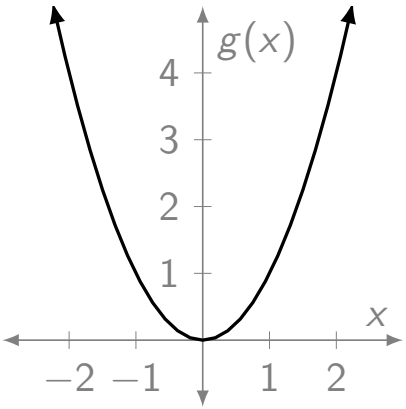


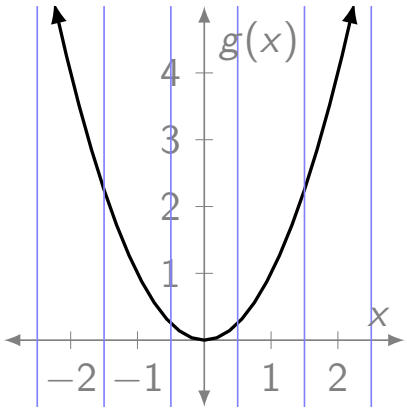
In the special case that $X = Y$ and we have $f : X \to X$, we can draw just one set of elements and represent the function as arrows pointing between elements in X. This is known as a directed graph, and we will investigate such structures further in Topic 5.

Coordinate graphs

Another way to represent functions visually is by using a coordinate graph. In a coordinate graph for a function $f : X \to Y$, the elements of X are listed along a horizontal axis, and the elements of Y are listed along a vertical axis. Elements (x, y) of the function are then marked as points at the coordinates corresponding with axis values x and y. This method of representation is particularly useful for cases where X and Y are each $\mathbb{R}$ or a subset of $\mathbb{R}$.

For example, for the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$, the function g can be represented with a coordinate graph as follows:





When given a coordinate graph, we can determine whether it represents a function by using the vertical line test: the graph represents a function if and only if every possible vertical line touches the graph at exactly one point.

Domain, codomain, and range

Definition. For a function $f : X \to Y$, the set of all input values X is called the domain of f, and the set of potential output values Y is called the codomain of f.

Definition. For a function $f : X \to Y$, the set of all output values actually obtained when evaluating all input values is called the range or image of f. The range of f can be denoted as $f(X)$ or $\text{range}(f)$ or $\text{im}(f)$. So the range of f is given by

$$f(X) = \{f(x) \ : \ x \in X\} \subseteq Y.$$

For example, again consider the sets $X = \{a, b, c\}$ and $Y = \{1, 2\}$, with function $f : X \to Y$ given by $f = \{(a, 1), (b, 2), (c, 2)\}$. Clearly the domain of f is X and the codomain of f is Y. Furthermore, the range of f is $\{1, 2\}$, which happens to be the same as the codomain in this case.

Consider also the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ for all $x \in \mathbb{R}$. Clearly the domain and codomain of g are both $\mathbb{R}$. The range of g is the set of all non-negative real numbers, so we have

$$\text{im}(g) = g(\mathbb{R}) = \{y \in \mathbb{R} \ : \ y \geq 0\}.$$

Image and pre-image

Definition. Suppose $f : X \to Y$ is a function and $A \subseteq X$. The image of A under f, written as $f(A)$, is the set of all output values attained by mapping all the input values in A under f. That is,

$$f(A) = \{f(x) \ : \ x \in A\} \subseteq Y.$$

Note that the image of the domain X under f is just the range (or image) of f, which justifies using the notation $f(X)$.

Definition. Suppose $f : X \to Y$ is a function and $B \subseteq Y$. The pre-image of B under f, written as $f^{-1}(B)$, is the set of all input values that map to the output values in B under f. That is,

$$f^{-1}(B) = \{x \in X \ : \ f(x) \in B\} \subseteq X.$$

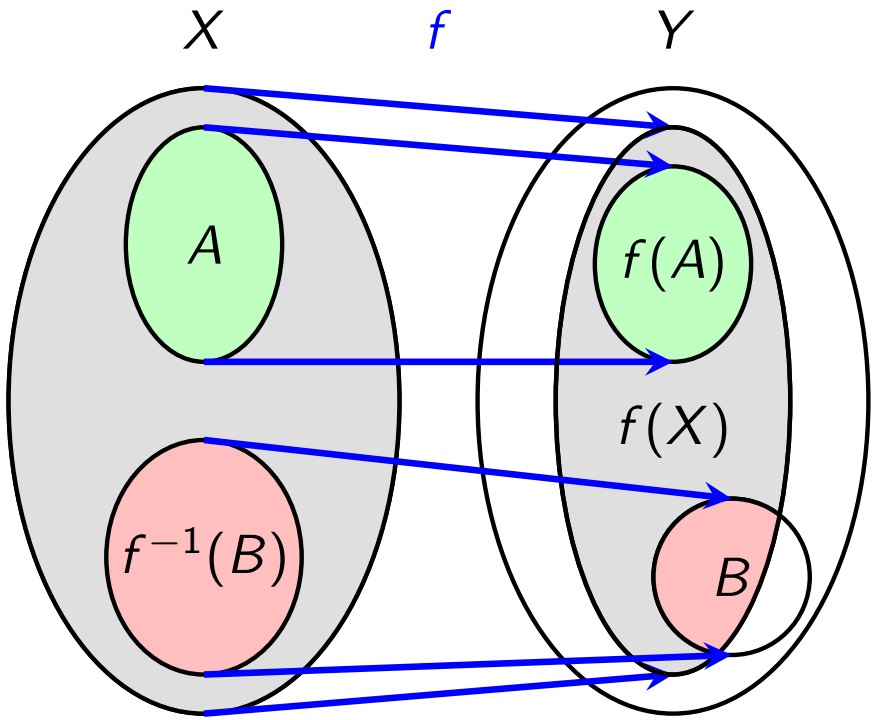
Consider again the example with sets $X = \{a, b, c\}$ and $Y = \{1, 2\}$, and function $f : X \to Y$ given by $f = \{(a, 1), (b, 2), (c, 2)\}$.
The image of $\{a, b\}$ under f is $f(\{a, b\}) = \{1, 2\}$, while $f(\{b, c\}) = \{2\}$.
The pre-image of $\{1\}$ under f is $f^{-1}(\{1\}) = \{a\}$, while $f^{-1}(\{2\}) = \{b, c\}$.

Consider also the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2$ for all $x \in \mathbb{R}$.
Then $g(\{-1, 0, 1\}) = \{0, 1\}$, while $g^{-1}(\{4, 9\}) = \{-3, -2, 2, 3\}$.

Venn and arrow diagrams

We can visualise images and pre-images for functions by adapting characteristics of Venn diagrams to our arrow diagrams.

For example, for a function $f : X \to Y$ with a subset of the domain $A \subseteq X$ and a subset of the codomain $B \subseteq Y$, we can draw the following:



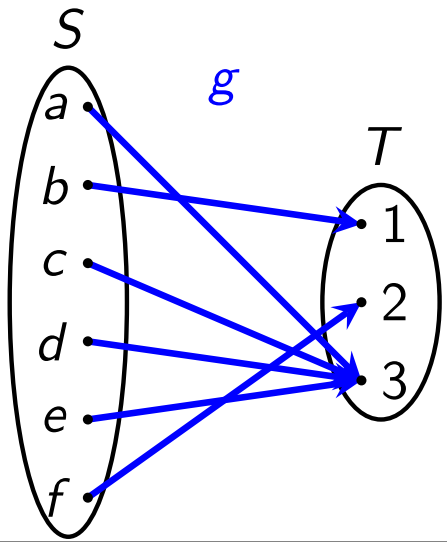
Example 1

Example. Suppose the students Altair, Bayek, Connor, Desmond, Ezio, and Frye are studying MATH1081 this term. Bayek is in tutorial 1, Frye is in tutorial 2, and the other four students are in tutorial 3.

(i) Define a function g that maps the students to their tutorials.
(ii) Draw the arrow diagram representing g.
(iii) Find the range of g.
(iv) Find the pre-image of each of the tutorials under g.

Solution. Labelling the students by their initials, we can define the set of students $S = \{a, b, c, d, e, f\}$ and the set of tutorials $T = \{1, 2, 3\}$. Then the function $g : S \to T$ that maps students to tutorials is given by the set $g = \{(a, 3), (b, 1), (c, 3), (d, 3), (e, 3), (f, 2)\}$.

The arrow diagram for g is provided to the right.



We can see from the diagram that the range of g is $g(S) = \{1, 2, 3\} = T$.

We can also see that the pre-images are given by

- $g^{-1}(\{1\}) = \{b\}$,
- $g^{-1}(\{2\}) = \{f\}$, and
- $g^{-1}(\{3\}) = \{a, c, d, e\}$.

Example 2

Example. Let the set $S = \{a, b, c, d, e, f\}$ represent the set of students Altair, Bayek, Connor, Desmond, Ezio, and Frye respectively. The function $h : S \to S$ mapping each student to their best friend is given by $h = \{(a, e), (b, f), (c, e), (d, e), (e, e), (f, b)\}$.

(i) Interpret this function h.

(ii) Draw the arrow diagram representing h.

(iii) Find the range of h.

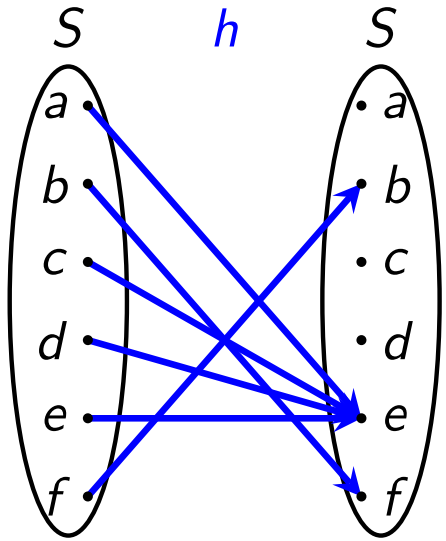
(iv) Find $h(\{a, c\})$ and $h^{-1}(\{a, c\})$.

Solution. Ezio is the best friend of Altair, Connor, Desmond, and himself. Bayek and Frye are each other's best friends.

The arrow diagram for h is provided to the right.

We can see from the diagram that the range of h is $h(S) = \{b, e, f\}$.

We can also see that $h(\{a, c\}) = \{e\}$ while $h^{-1}(\{a, c\}) = \{\}$.



Floor and ceiling functions

Definition. The floor function is a function with domain $\mathbb{R}$ and codomain $\mathbb{Z}$ defined as follows: for any $x \in \mathbb{R}$, the floor of x is written as $\lfloor x \rfloor$ and is given by the largest integer less than or equal to x.

Definition. The ceiling function is a function with domain $\mathbb{R}$ and codomain $\mathbb{Z}$ defined as follows: for any $x \in \mathbb{R}$, the ceiling of x is written as $\lceil x \rceil$ and is the smallest integer greater than or equal to x.

Example. Evaluate the following:

- $\lfloor 3.14 \rfloor = 3$.
- $\lceil 3.14 \rceil = 4$.
- $\lfloor -0.5 \rfloor = -1$.
- $\lceil -0.5 \rceil = 0$.
- $\lfloor 1 \rfloor = 1$.
- $\lceil 1 \rceil = 1$.

Example 3

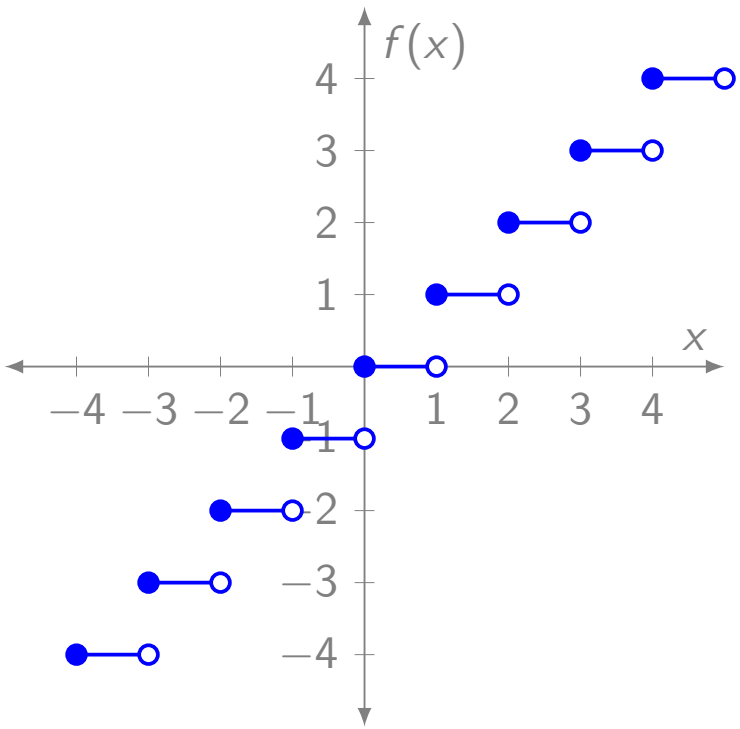
Example. Let $f : \mathbb{R} \to \mathbb{R}$ be the function given by $f(x) = \lfloor x \rfloor$, and let $g : \mathbb{R} \to \mathbb{R}$ be the function given by $g(x) = \lceil x \rceil$.

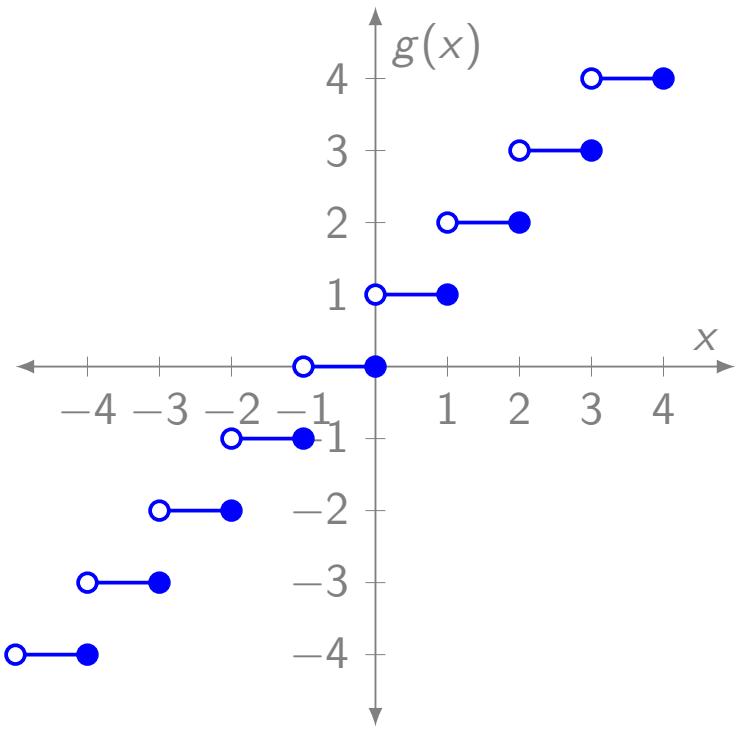
(i) Draw the coordinate graphs representing f and g.

(ii) Find the range of f and of g.

(iii) Let $S = \{\frac{1}{n} \ : \ n \in \mathbb{Z}^+\} = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$. Find each of $f(S)$, $g(S)$, $f^{-1}(S)$, and $g^{-1}(S)$.

Solution. The coordinate graphs are provided below.





Example 3 (continued)

Example. Let $f : \mathbb{R} \to \mathbb{R}$ be the function given by $f(x) = \lfloor x \rfloor$, and let $g : \mathbb{R} \to \mathbb{R}$ be the function given by $g(x) = \lceil x \rceil$.

(i) Draw the coordinate graphs representing f and g.

(ii) Find the range of f and of g.

(iii) Let $S = \{\frac{1}{n} \ : \ n \in \mathbb{Z}^+\} = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$. Find each of $f(S)$, $g(S)$, $f^{-1}(S)$, and $g^{-1}(S)$.

Solution. The coordinate graphs indicate that the range of both f and of g is $\mathbb{Z}$. To confirm this, notice that for any $k \in \mathbb{Z}$, we have $f(k) = g(k) = k$, so there is at least one input value that returns any integer k as an output.

Notice that $f(S) = \{f(1), f(\frac{1}{2}), f(\frac{1}{3}), f(\frac{1}{4}), \dots\} = \{1, 0, 0, 0, \dots\} = \{0, 1\}$.

Similarly, $g(S) = \{g(1), g(\frac{1}{2}), g(\frac{1}{3}), g(\frac{1}{4}), \dots\} = \{1, 1, 1, 1, \dots\} = \{1\}$.

Since the range of both f and of g is $\mathbb{Z}$, no input value can return a non-integer output. So in particular, the pre-image of any non-integer is empty, that is, $f(\frac{1}{2}) = g(\frac{1}{2}) = \{\}$, $f(\frac{1}{3}) = g(\frac{1}{3}) = \{\}$, and so on.

So $f^{-1}(S) = f^{-1}(\{1, \frac{1}{2}, \frac{1}{3}, \dots\}) = f^{-1}(\{1\}) = \{x \in \mathbb{R} \ : \ 1 \leq x < 2\}$.

Similarly, $g^{-1}(S) = g^{-1}(\{1, \frac{1}{2}, \frac{1}{3}, \dots\}) = g^{-1}(\{1\}) = \{x \in \mathbb{R} \ : \ 0 < x \leq 1\}$.

UNSW SYDNEY

MATH1081 – Discrete Mathematics

Topic 1 – Set theory and functions
Lecture 1.06 – Properties of functions and inverses

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

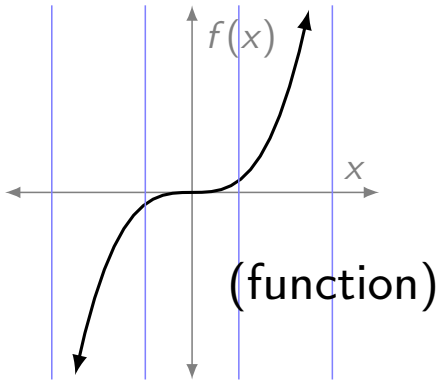
Functions (again)

Recall that a set $f \subseteq X \times Y$ is a function if and only if there is exactly one ordered pair $(x, y) \in f$ for each $x \in X$.

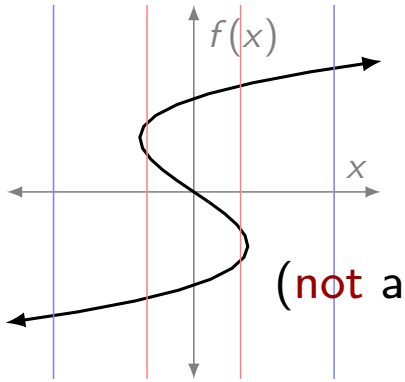
Equivalently, we could say that a set $f \subseteq X \times Y$ is a function if and only if every possible input value in X has exactly one corresponding output value in Y. That is, a set $f \subseteq X \times Y$ is a function if and only if for every $x \in X$, there is exactly one $y \in Y$ such that $f(x) = y$.

In terms of arrow diagrams, a set $f \subseteq X \times Y$ is a function if and only if each element of the domain X has exactly one outgoing arrow.

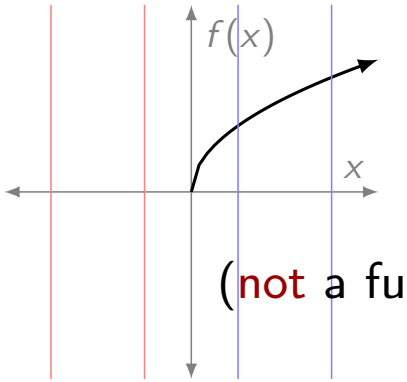
In terms of coordinate graphs, a set $f \subseteq \mathbb{R} \times \mathbb{R}$ is a function if and only if every possible vertical line touches the graph at exactly one point.



(function)



(not a function)



(not a function)

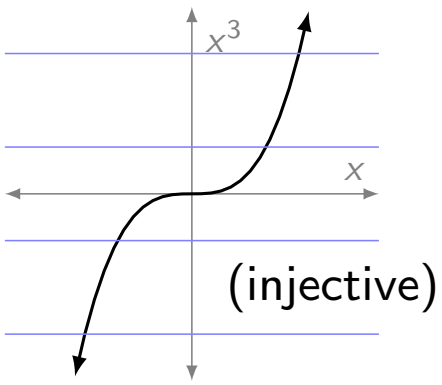
Injectivity

Definition. A function $f : X \to Y$ is injective (or one-to-one) if and only if every possible output value in Y has at most one corresponding input value in X. Equivalently, a function $f : X \to Y$ is injective if and only if any of the following are true:

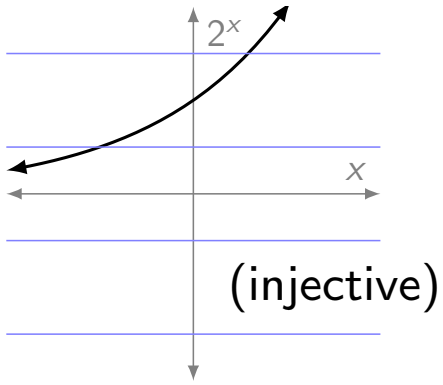
- For every $y \in Y$, there is at most one $x \in X$ such that $f(x) = y$.
- For every $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then we must have that $x_1 = x_2$.
- For every $x_1, x_2 \in X$, if $x_1 \neq x_2$ then we must have that $f(x_1) \neq f(x_2)$.

In terms of arrow diagrams, a function $f : X \to Y$ is injective if and only if each element of the codomain Y has at most one incoming arrow.

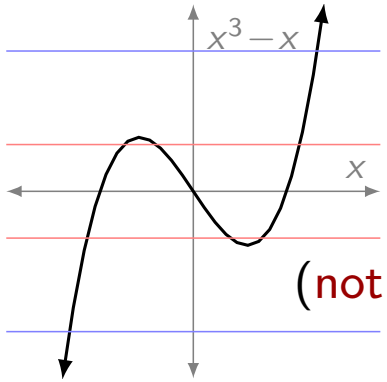
In terms of coordinate graphs, a function $f : \mathbb{R} \to \mathbb{R}$ is injective if and only if every possible horizontal line touches the graph at at most one point.



(injective)



(injective)



(not injective)

Injectivity – examples

Example. Decide whether each function below is injective, and prove your claim.

- $f : \{1, 2, 3\} \to \{1, 2, 3, 4\}$, $f = \{(1, 2), (2, 3), (3, 4)\}$ is injective since for every possible output value (1, 2, 3, 4), there is at most one corresponding input value (none, 1, 2, 3 respectively).
- $f : \{1, 2, 3\} \to \{1, 2, 3, 4\}$, $f = \{(1, 2), (2, 4), (3, 2)\}$ is not injective since there is an output value with more than one corresponding input value. Specifically, $f(1) = 2 = f(3)$ but $1 \neq 3$.
- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$ is not injective since there exists an output value with more than one corresponding input value. For example, $2 \neq -2$ but $f(2) = 4 = f(-2)$.
- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2x + 1$ is injective since for every $x_1, x_2 \in \mathbb{Z}$, if $f(x_1) = f(x_2)$ then we have $2x_1 + 1 = 2x_2 + 1$, which after rearrangement implies $x_1 = x_2$.

  Notice that to prove a function is injective when its domain is infinite (or very large), we need to give a proof for arbitrary domain elements x_1 and x_2.

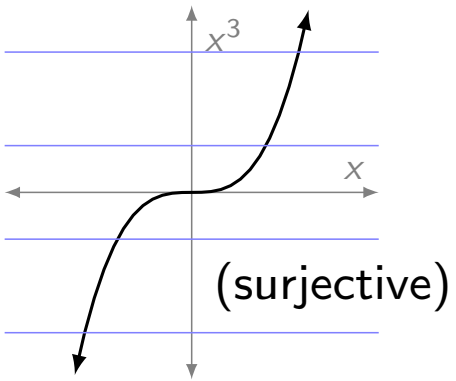
Surjectivity

Definition. A function $f : X \to Y$ is surjective (or onto) if and only if every possible output value in Y has at least one corresponding input value in X. Equivalently, a function $f : X \to Y$ is surjective if and only if any of the following are true:

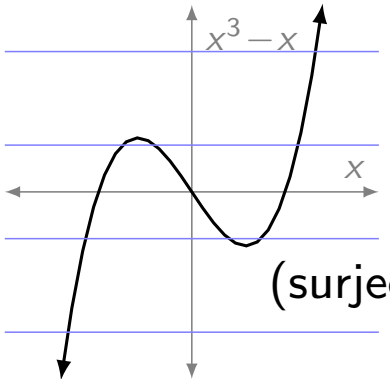
- For every $y \in Y$, there is at least one $x \in X$ such that $f(x) = y$.
- The range of f and the codomain of f are equal, that is, $f(X) = Y$.

In terms of arrow diagrams, a function $f : X \to Y$ is surjective if and only if each element of the codomain Y has at least one incoming arrow.

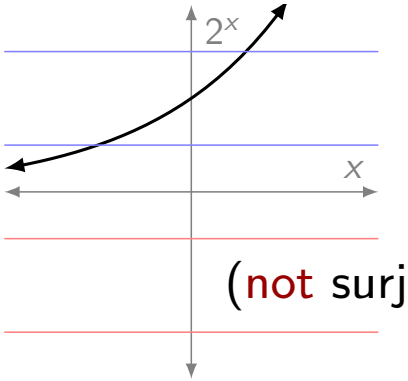
In terms of coordinate graphs, a function $f : \mathbb{R} \to \mathbb{R}$ is surjective if and only if every possible horizontal line touches the graph at at least one point.



(surjective)



(surjective)



(not surjective)

Surjectivity – examples

Example. Decide whether each function below is surjective, and prove your claim.

- $f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$, $f = \{(1, 2), (2, 3), (3, 1), (4, 2)\}$ is surjective since for every possible output value (1, 2, 3), there is at least one corresponding input value (3, 1 and 4, 2 respectively).
- $f : \{1, 2, 3, 4\} \to \{1, 2, 3\}$, $f = \{(1, 1), (2, 2), (3, 1), (4, 2)\}$ is not surjective since there is an output value with less than one corresponding input value. Specifically, 3 is in the codomain but $f(x) = 3$ has no solution for any $x \in \{1, 2, 3, 4\}$.
- $f : \mathbb{N} \to \mathbb{N}$, $f(x) = x^2$ is not surjective since there exists an output value with less than one corresponding input value. For example, $2 \in \mathbb{Z}$ but $f(x) = 2$ has no solution for any $x \in \mathbb{Z}$.
- $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 2 - x$ is surjective since for every $y \in \mathbb{Z}$, the equation $f(x) = y$ has a solution for some $x \in \mathbb{Z}$, namely $x = 2 - y$.

  Notice that to prove a function is surjective when its codomain is infinite (or very large), we need to give a proof for an arbitrary codomain element y.

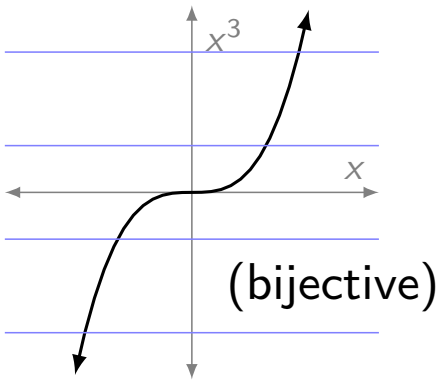
Bijectivity

Definition. A function $f : X \to Y$ is bijective (or a one-to-one correspondence) if and only if every possible output value in Y has exactly one corresponding input value in X. Equivalently, a function $f : X \to Y$ is bijective if and only if any of the following are true:

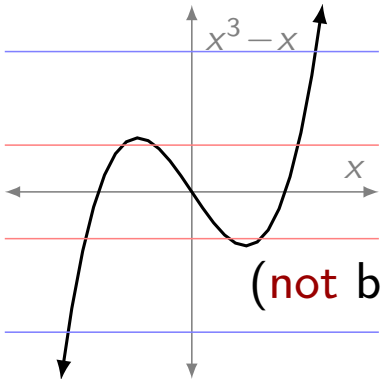
- For every $y \in Y$, there is exactly one $x \in X$ such that $f(x) = y$.
- The function f is both injective and surjective.

In terms of arrow diagrams, a function $f : X \to Y$ is bijective if and only if each element of the codomain Y has exactly one incoming arrow.

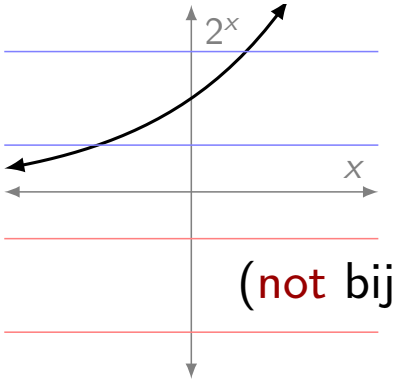
In terms of coordinate graphs, a function $f : \mathbb{R} \to \mathbb{R}$ is bijective if and only if every possible horizontal line touches the graph at exactly one point.



(bijective)



(not bijective)



(not bijective)

Cardinalities of domain and codomain

Theorem. Suppose $f : X \to Y$ is a function for some sets X and Y.

- If f is injective, then $|X| \leq |Y|$.
- If f is surjective, then $|X| \geq |Y|$.
- If f is bijective, then $|X| = |Y|$.

Proof. For ease of reference, we describe f in terms of its arrow diagram representation. Since f is a function, we know there must be exactly one outgoing arrow for each element in the domain, so there are exactly $|X|$ arrows in the diagram.

If f is injective, then there must be at most one incoming arrow for each element in the codomain, so there are at least $|X|$ elements in the codomain.

If f is surjective, then there must be at least one incoming arrow for each element in the codomain, so there are at most $|X|$ elements in the codomain.

If f is bijective, then f is both injective and surjective, meaning both $|X| \leq |Y|$ and $|X| \geq |Y|$, so we must have that $|X| = |Y|$.

Notice that the converse (opposite direction) statements are not true in general. For example, if $|X| \leq |Y|$ then this does not guarantee that $f : X \to Y$ is injective.

Function composition

Definition. Given two functions $f : X \to Y$ and $g : Y \to Z$ for any sets X, Y, Z, the composition of f and g is the function $g \circ f : X \to Z$ defined by

$$(g \circ f)(x) = g(f(x)) \quad \text{for all } x \in X.$$

More generally, the composition of functions f and g is defined whenever the range of f is a subset of the domain of g.

Notice that the order in which the component functions are applied is from right to left, since applying $g \circ f$ to x returns the result of applying f to x and then g to this output.

Example. Suppose $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ are functions defined by $f(x) = x^2$ and $g(x) = 2 - x$. Find $g \circ f$ and $f \circ g$.

Solution. For all $x \in \mathbb{Z}$, we have $(g \circ f)(x) = g(f(x)) = g(x^2) = 2 - x^2$, while $(f \circ g)(x) = f(g(x)) = f(2 - x) = (2 - x)^2 = 4 - 4x + x^2$.

Theorem. Given two functions $f : X \to Y$ and $g : Y \to Z$:

- if f and g are both injective, then $g \circ f$ is also injective.
- if f and g are both surjective, then $g \circ f$ is also surjective.

Proof. Try this yourself! (See tutorial Problem Set 1, Question 34.)

Identity and inverse functions

Definition. For any set X, the identity function for X, denoted ι_X (Greek letter iota) or id_X, is the function $\iota_X : X \to X$ defined by $\iota_X(x) = x$ for all $x \in X$.

Theorem. For any function $f : X \to Y$, we have $f \circ \iota_X = f$ and $\iota_Y \circ f = f$.

Proof. For all $x \in X$, we have $(f \circ \iota_X)(x) = f(\iota_X(x)) = f(x)$.
Similarly for all $x \in X$, we have $(\iota_Y \circ f)(x) = \iota_Y(f(x)) = f(x)$.

Definition. The inverse of a function $f : X \to Y$, if it exists, is the function $g : Y \to X$ satisfying $g \circ f = \iota_X$ and $f \circ g = \iota_Y$. That is, $(g \circ f)(x) = x$ for all $x \in X$, and $(f \circ g)(y) = y$ for all $y \in Y$.

Notation. We write f^{-1} for the inverse of f (if it exists). This looks the same as our notation for the pre-image of a set, but we can distinguish the two notations by the fact that the inverse function takes elements of Y as inputs, whereas the pre-image takes subsets of Y as inputs.

Properties of inverses

In terms of sets of ordered pairs, if $f \subseteq X \times Y$ is a function and its inverse f^{-1} exists, then $f^{-1} = \{(y, x) \in Y \times X \ : \ (x, y) \in f\}$. This justifies the following properties of the inverse function:

Lemma. If a function f has an inverse, its inverse must be unique.

Proof. It is clear that given any function $f \subseteq X \times Y$, its inverse f^{-1} is defined uniquely as a subset of $Y \times X$ in terms of f.

Lemma. If a function f has an inverse f^{-1}, then the inverse of f^{-1} is f. That is, $(f^{-1})^{-1} = f$.

Proof. Suppose $f \subseteq X \times Y$ has inverse $f^{-1} = \{(y, x) \ : \ (x, y) \in f\}$. Then $(f^{-1})^{-1} = \{(x, y) \ : \ (y, x) \in f^{-1}\} = \{(x, y) \ : \ (x, y) \in f\} = f$.

Theorem. Suppose $f : X \to Y$ and $g : Y \to Z$ are functions such that their composition $g \circ f$ has an inverse. Then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. Let $h = f^{-1} \circ g^{-1}$. Then we have

$$h \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f = f^{-1} \circ \iota_Y \circ f = f^{-1} \circ f = \iota_X,$$

$$(g \circ f) \circ h = g \circ (f \circ f^{-1}) \circ g^{-1} = g \circ \iota_X \circ g^{-1} = g \circ g^{-1} = \iota_Y.$$

So indeed h is the unique inverse of $g \circ f$, that is, $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Finding inverses

If the output values of $f : X \to Y$ are defined by a formula $y = f(x)$ for all $x \in X$, then if the inverse f^{-1} exists, it satisfies the formula $x = f^{-1}(y)$ for all $y \in Y$.

Example. Find the inverse, if it exists, of the following functions.

- $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 1$.

  Solution. We write $y = 2x + 1$ and rearrange to make x the subject, giving $x = \frac{y-1}{2}$. So the inverse $f^{-1} : \mathbb{R} \to \mathbb{R}$ exists and is given by $f^{-1}(y) = \frac{y-1}{2}$. (Or equivalently, $f^{-1}(x) = \frac{x-1}{2}$.)

- $g : \mathbb{Z} \to \mathbb{Z}$, $g(x) = 2x + 1$.

  Solution. If the inverse exists, it is given by $g^{-1} : \mathbb{Z} \to \mathbb{Z}$, $g^{-1}(y) = \frac{y-1}{2}$. But this formula returns non-integer outputs for even integer inputs, so it is not well-defined. So the inverse function does not exist.

- $h : \mathbb{R} \to \mathbb{R}^+$, $h(x) = x^2$.

  Solution. Writing $y = x^2$ and rearranging to make x the subject gives $x = \pm\sqrt{y}$. So if the inverse of h exists, it is given by $h^{-1} : \mathbb{R}^+ \to \mathbb{R}$, $h^{-1}(x) = \pm\sqrt{x}$. But this formula returns more than one output for any positive real input, so it is not well-defined as a function. So the inverse function does not exist.

Inverses and bijective functions

Theorem. The inverse of a function $f : X \to Y$ exists if and only if f is bijective.

Proof. For ease of reference, we describe f and f^{-1} in terms of their arrow diagram representations. Since f is a function, we know there must be exactly one outgoing arrow for each element in the domain X.

Proof that if its inverse function exists, then f must be bijective:
The arrow diagram representation for the inverse function f^{-1} is formed by reversing the direction of all the arrows in the arrow diagram for f. Since $f^{-1} : Y \to X$ is a function, every element of Y must have exactly one outgoing arrow. This means that in the arrow diagram for f, every element of Y must have exactly one incoming arrow. So f is bijective.

Proof that if f is bijective, then it must have an inverse function:
Since it is bijective, the arrow diagram for f must have exactly one incoming arrow for every element in Y. Reversing the direction of all the arrows in the diagram will create a representation for a new function $g : Y \to X$, since every element in its domain Y will have exactly one outgoing arrow. Furthermore, this function g must be the inverse of f, since $g(f(x)) = x$ for all $x \in X$ and $f(g(y)) = y$ for all $y \in Y$.

Laws of set algebra

For any sets A, B, C with universal set $\mathcal{U}$ and empty set $\varnothing$, we have the following laws of set algebra:

Commutativity:

$$A \cup B = B \cup A,$$
$$A \cap B = B \cap A.$$

Associativity:

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

Distributivity:

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

Absorption:

$$A \cup (A \cap B) = A,$$
$$A \cap (A \cup B) = A.$$

Idempotence:

$$A \cup A = A,$$
$$A \cap A = A.$$

Identity:

$$A \cup \varnothing = A,$$
$$A \cap \mathcal{U} = A.$$

Domination:

$$A \cup \mathcal{U} = \mathcal{U},$$
$$A \cap \varnothing = \varnothing.$$

Complement law:

$$A \cup A^c = \mathcal{U},$$
$$A \cap A^c = \varnothing.$$

Double complement law:

$$(A^c)^c = A.$$

De Morgan's law:

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

We also have the following definitions:

Difference:

$$A - B = A \cap B^c.$$

Symmetric difference:

$$A \ominus B = (A \cup B) - (A \cap B).$$