

Cambridge University Press
978-1-107-02753-4 - Digital Logic Design: A Rigorous Approach
Guy Even and Moti Medina
Excerpt
[More information](#)

PART I

PRELIMINARIES

Cambridge University Press
978-1-107-02753-4 - Digital Logic Design: A Rigorous Approach
Guy Even and Moti Medina
Excerpt
[More information](#)

CHAPTER 1 Sets and Functions

This chapter introduces two major notions: sets and functions. We are all familiar with real functions, for example, $f(x) = 2x + 1$ and $g(x) = \sin(x)$. Here the approach is somewhat different. The first difference is that we do not limit the discussion to the set of real numbers; instead, we consider arbitrary sets and are mostly interested in sets that contain only a finite number of elements. The second difference is that we do not define a “rule” for assigning a value for each x ; instead, a function is simply a list of pairs (x, y) , where y denotes the value of the function when the argument equals x . The definition of functions relies on the definitions of sets and relations over sets. That is why we need to define various operations over sets such as union, intersection, complement, and Cartesian product.

The focus of this book is Boolean functions. Boolean functions are a special family of functions. Their arguments and values are finite sequences of 0 and 1 (also called bits). In this chapter, we show how to represent a Boolean function by a truth table and multiplication tables. Other representations presented later in the book are Boolean formulas and combinational circuits.

1.1 SETS

A *set* is a collection of objects. When we deal with sets, we usually have a *universal set* that contains all the possible objects. In this section, we denote the universal set by U .

The universal set need not be fixed. For example, when we consider real numbers, the universal set is the set of real numbers. Similarly, when we consider natural numbers, the universal set is the set of natural numbers. The universal set need not be comprised only of abstract objects such as numbers. For example, when we consider people, the universal set is the set of all people.

One way to denote a set is by listing the objects that belong to the set and delimiting them by curly brackets. For example, suppose the universe is the set of integers, and consider the set $A = \{1, 5, 12\}$. Then 1 is in A , but 2 is not in A . An object that belongs to a set is called an *element*. We denote the fact that 1 is in A by $1 \in A$ and the fact that 2 is not in A by $2 \notin A$.

Definition 1.1 Consider two sets A and B .

1. We say that A is a *subset* of B if every element in A is also an element in B . We denote that A is a subset of B by $A \subseteq B$.
2. We say that A *equals* B if the two sets consist of exactly the same elements, formally, if $A \subseteq B$ and $B \subseteq A$. We denote that A and B are equal sets by $A = B$.
3. The *union* of A and B is the set C such that every element of C is an element of A or an element of B . We denote the union of A and B by $A \cup B$.
4. The *intersection* of A and B is the set C such that every element of C is an element of A and an element of B . We denote the intersection of A and B by $A \cap B$.
5. The *difference* A and B is the set C such that every element of C is an element of A and not an element of B . We denote the difference of A and B by $A \setminus B$.

The *empty set* is a very important set (as important as the number zero).

Definition 1.2 The empty set is the set that does not contain any element. It is usually denoted by \emptyset .

Sets are often specified by a condition or a property. This means that we are interested in all the objects in the universal set that satisfy a certain property. Let P denote a property. We denote the set of all elements that satisfy property P as follows:

$$\{x \in U \mid x \text{ satisfies property } P\}.$$

The preceding notation should be read as follows: the set of all elements x in the universal set U such that x satisfies property P .

Every set we consider is a subset of the universal set. This enables us to define the complement of a set as follows.

Definition 1.3 The *complement* of a set A is the set $U \setminus A$. We denote the complement set of A by \bar{A} .

Given a set A , we can consider the set of all its subsets.

Definition 1.4 The *power set* of a set A is the set of all the subsets of A . The power set of A is denoted by $P(A)$ or 2^A .

We can pair elements together to obtain ordered pairs.

Definition 1.5 Two objects (possibly equal) with an order (i.e., the first object and the second object) are called an *ordered pair*. We denote an ordered pair by (x, y) . This notation means that x is the first object in the pair and y is the second object in the pair.

Consider two ordered pairs (x, y) and (x', y') . We say that $(x, y) = (x', y')$ if $x = x'$ and $y = y'$.

We usually refer to the first object in an ordered pair as the first *coordinate*. The second object is referred to as the second coordinate.

An important method to build large sets from smaller ones is by the *Cartesian product*.

Definition 1.6 The *Cartesian product* of the sets A and B is the set

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

Every element in a Cartesian product is an ordered pair. Thus the Cartesian product $A \times B$ is simply the set of ordered pairs (a, b) such that the first coordinate is in A and the second coordinate is in B . The Cartesian product $A \times A$ is denoted by A^2 .

The definition of ordered pairs is extended to tuples, as follows.

Definition 1.7 A k -tuple is a set of k objects with an order. This means that a k -tuple has k coordinates numbered $\{1, \dots, k\}$. For each coordinate i , there is an object in the i th coordinate.

An ordered pair is a 2-tuple. A k -tuple is denoted by (x_1, \dots, x_k) , where the element in the i th coordinate is x_i . Tuples are compared in each coordinate, thus $(x_1, \dots, x_k) = (x'_1, \dots, x'_k)$ if and only if $x_i = x'_i$ for every $i \in \{1, \dots, k\}$.

We also extend the definition of Cartesian products to products of k sets, as follows.

Definition 1.8 The *Cartesian product* of the sets A_1, A_2, \dots, A_k is the set

$$A_1 \times A_2 \times \dots \times A_k \triangleq \{(a_1, \dots, a_k) \mid a_i \in A_i \text{ for every } 1 \leq i \leq k\}.$$

The Cartesian product of k copies of A is denoted by A^k .

EXAMPLES

0*. **Russell's paradox.** A formal axiomatic development of set theory is a branch of logic called *axiomatic set theory*. This branch developed in response to paradoxes in set theory. One of the most famous paradoxes was discovered by Bertrand Russell in 1901.

Suppose we do not restrict ourselves to a subset of a universal set. Consider the set Z defined by

$$Z \triangleq \{x \mid x \notin x\},$$

namely, an object x is in Z if and only if it does not contain itself as an element.

Russell's paradox is obtained as follows. Is $Z \in Z$? If $Z \in Z$, then because every element $x \in Z$ satisfies $x \notin x$, we conclude that $Z \notin Z$ —a contradiction. So we are left with the complementary option that $Z \notin Z$. But if $Z \notin Z$, then Z satisfies the only condition for being a member of Z . Thus $Z \in Z$ —again, a contradiction.

- Examples of sets: (i) $A \triangleq \{1, 2, 4, 8\}$, the universal set is the set of numbers; (ii) $B \triangleq \{\text{pencil, pen, eraser}\}$, the universal set is the set of “the things that we have in our pencil case.”
- Examples of subsets of $A \triangleq \{1, 2, 4, 8\}$ and $B \triangleq \{\text{pencil, pen, eraser}\}$: (i) $\{1, 2, 4, 8\} \subseteq A$; (ii) $\{1, 2, 8\} \subseteq A$; (iii) $\{1, 2, 4\} \subseteq A$; (iv) $\{1, 2\} \subseteq A$; (v) $\{1\} \subseteq A$; (vi) $\emptyset \subseteq A$; (vii) $\{\text{pen}\} \subseteq B$.
- Examples of equal sets. Let $A \triangleq \{1, 2, 4, 8\}$ and $B \triangleq \{\text{pencil, pen, eraser}\}$: (i) order and repetitions do not affect the set, e.g., $\{1, 1, 1\} = \{1\}$ and $\{1, 2\} = \{2, 1\}$; (ii) $\{2, 4, 8, 1, 1, 2\} = A$; (iii) $\{1, 2, 44, 8\} \neq A$; (iv) $A \neq B$.
- We claim that $\emptyset \subseteq X$ for every set X . By Item 1 in Definition 1.1, we need to prove that every element in \emptyset is also in X . Because the empty set \emptyset does not contain any element (see Definition 1.2), all the elements in \emptyset are also in X , as required.

5. The empty set is denoted by \emptyset . The set $\{\emptyset\}$ contains a single element, which is the empty set. Therefore $\emptyset \in \{\emptyset\}$ but $\emptyset \neq \{\emptyset\}$. Because $\emptyset \subseteq X$ for all set X (see Example 4), $\emptyset \in \{\emptyset\}$ and $\emptyset \subseteq \{\emptyset\}$.
6. Examples of unions: (i) $\{1, 2, 4, 8\} \cup \{1, 2, 4\} = A$; (ii) $\{1, 2\} \cup \{4\} \neq A$; (iii) $A \cup \emptyset = A$; (iv) $A \cup B = \{1, 2, 4, 8, \text{pencil, pen, eraser}\}$.
7. Intersection of sets: (i) $\{1, 2, 4\} \cap A = \{1, 2, 4\}$; (ii) $\{8, 16, 32\} \cap A = \{8\}$; (iii) $\{16, 32\} \cap A = \emptyset$; (iv) $A \cap \emptyset = \emptyset$; (v) $A \cap B = \emptyset$; (vi) for every two sets X and Y , $X \cap Y \subseteq X$.
8. Suppose the universal set is the set of real numbers \mathbb{R} . We can define the following sets:

- (i) The set of integers \mathbb{Z} is the set of all reals that are multiples of 1; that is,

$$\begin{aligned}\mathbb{Z} &\triangleq \{x \in \mathbb{R} \mid x \text{ is a multiple of } 1\} \\ &= \{0, +1, -1, +2, -2, \dots\}.\end{aligned}$$

- (ii) The set of natural numbers \mathbb{N} is the set of all nonnegative integers; that is,

$$\begin{aligned}\mathbb{N} &\triangleq \{x \in \mathbb{R} \mid x \in \mathbb{Z} \text{ and } x \geq 0\} \\ &= \{0, 1, 2, 3, \dots\}.\end{aligned}$$

- (iii) The set of positive natural numbers \mathbb{N}^+ is the set of all positive integers; that is,

$$\begin{aligned}\mathbb{N}^+ &\triangleq \{x \in \mathbb{R} \mid x \in \mathbb{Z} \text{ and } x > 0\} \\ &= \{1, 2, 3, \dots\}.\end{aligned}$$

- (iv) The set of positive real numbers is denoted by \mathbb{R}^+ ; that is,

$$\mathbb{R}^+ \triangleq \{x \in \mathbb{R} \mid x > 0\}.$$

- (v) The set of nonnegative real numbers is denoted by \mathbb{R}^{\geq} ; that is,

$$\mathbb{R}^{\geq} \triangleq \{x \in \mathbb{R} \mid x \geq 0\}.$$

9. If $A \cap B = \emptyset$, then we say that A and B are *disjoint*. We say that the sets A_1, \dots, A_k are disjoint if $A_1 \cap \dots \cap A_k = \emptyset$. We say that the sets A_1, \dots, A_k are *pairwise-disjoint* if, for every $i \neq j$, the sets A_i and A_j are disjoint.
10. Consider the three sets $\{1, 2\}$, $\{2, 3\}$, and $\{1, 3\}$. Their intersection is empty; therefore they are disjoint. However, the intersection of every pair of sets is nonempty; therefore they are not pairwise disjoint.
11. When A and B are disjoint, that is, $A \cap B = \emptyset$, we denote their union by $A \cup B$: (i) $\{1, 2\} \cup \{4, 8\} = A$; (ii) $\{1, 2\} \cup A = A$.
12. Difference of sets: (i) $\{1, 2\} \setminus \{2, 4\} = \{1\}$; (ii) $A \setminus \emptyset = A$; (iii) $A \setminus A = \emptyset$; (iv) $A \setminus B = A$.
13. Formal specification of union, intersection, and difference:
 - (i) $A \cup B \triangleq \{x \in U \mid x \in A \text{ or } x \in B\}$
 - (ii) $A \cap B \triangleq \{x \in U \mid x \in A \text{ and } x \in B\}$
 - (iii) $A \setminus B \triangleq \{x \in U \mid x \in A \text{ and } x \notin B\}$
14. We claim that $\bar{A} = \{x \in U \mid x \notin A\}$. Indeed, $x \in \bar{A}$ is shorthand for $x \in U \setminus A$, where U is the universe. Hence $x \in \bar{A}$ if and only if $x \in U$ and $x \notin A$, as required.

15. **Contraposition.** In this example, we discuss a logical equivalence between two statements, called *contraposition*. A rigorous treatment of contraposition appears in Chapter 6. Consider the following two statements (regarding sets A and B):

- $A \subseteq B$
- $\bar{B} \subseteq \bar{A}$

We show that these two statements are equivalent. Assume that $A \subseteq B$. By definition, this means that

$$\forall x \in U : x \in A \Rightarrow x \in B. \quad (1.1)$$

Now we wish to show that $\bar{B} \subseteq \bar{A}$. For the sake of contradiction, assume that there exists an element x for which $x \in \bar{B}$ and $x \notin \bar{A}$. This means that $x \notin B$ and $x \in A$. But this contradicts Eq. 1.1. Hence $\bar{B} \subseteq \bar{A}$, as required.

Assume that $\bar{B} \subseteq \bar{A}$. By the preceding proof, it follows that $\bar{\bar{A}} \subseteq \bar{\bar{B}}$. Note that $\bar{\bar{A}} = A$ and $\bar{\bar{B}} = B$. Hence $A \subseteq B$, as required.

In its general form, contraposition states that the statement $P \Rightarrow Q$ is logically equivalent to the statement $\text{NOT}(Q) \Rightarrow \text{NOT}(P)$. The proof of this equivalence is similar to the preceding proof.

16. Operations on sets defined in Definition 1.1 can be depicted using *Venn diagrams*. The idea is to depict each set as a region defined by a closed curve in the plane. For example, a set can be depicted by a disk. Elements in the set are represented by points in the disk, and elements not in the set are represented by points outside the disk. The intersections between regions partition the planes into *cells*, where each cell represents an intersection of sets and complements of sets. In Figure 1.1, we depict the union, intersection, difference, and complement of two sets A and B that are subsets of a universal set U .
17. We claim that $A \setminus B = A \cap \bar{B}$. To prove this, we show containment in both directions. (i) We prove that $A \setminus B \subseteq A \cap \bar{B}$. Let $x \in A \setminus B$. By the definition of subtraction of sets, this means that $x \in A$ and $x \notin B$. By the definition of a complement set, $x \in \bar{B}$. By the definition of intersection, $x \in A \cap \bar{B}$, as required. (ii) We prove that $A \cap \bar{B} \subseteq A \setminus B$. Let $x \in A \cap \bar{B}$. By the definition of intersection of sets, this means that $x \in A$ and $x \in \bar{B}$. By the definition a complement set, $x \in \bar{B}$ implies that $x \notin B$. By the definition of subtraction, $x \in A \setminus B$, as required.
18. Let X denote a set with a finite number of elements. The size of a set X is the number of elements in X . The size of a set is also called its *cardinality*. The size of a set X is denoted by $|X|$: (i) $|A| = 4$; (ii) $|B| = 3$; (iii) $|A \cup B| = 7$; (iv) if X and Y are disjoint finite sets, then $|X \cup Y| = |X| + |Y|$.
19. The power set of $A = \{1, 2, 4, 8\}$ is the set of all subsets of A , namely,

$$\begin{aligned} P(A) = \{ & \emptyset, \{1\}, \{2\}, \{4\}, \{8\}, \\ & \{1, 2\}, \{1, 4\}, \{1, 8\}, \{2, 4\}, \{2, 8\}, \{4, 8\}, \\ & \{1, 2, 4\}, \{1, 2, 8\}, \{2, 4, 8\}, \{1, 4, 8\}, \\ & \{1, 2, 4, 8\} \}. \end{aligned}$$

20. Every element of the power set $P(A)$ is a subset of A , and every subset of A is an element of $P(A)$.

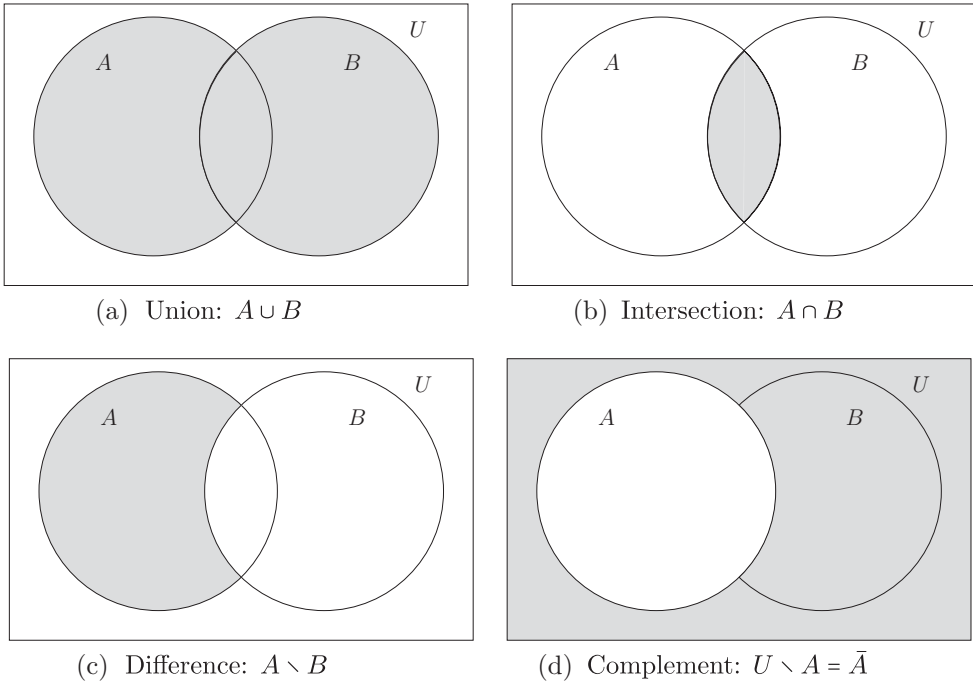


Figure 1.1. Venn diagrams over the sets A and B with respect to the universal set U .

21. Recall that for every set X , the empty set \emptyset is a subset of X (see Example 4). It follows that $\emptyset \in P(X)$ for every set X . In particular, $\emptyset \in P(\emptyset)$.
22. How many subsets does the set A have? By counting the list in Example 19, we see that $|P(A)| = 16$. As we will see later in Problem 2.6, in general, $|P(A)| = 2^{|A|}$. This justifies the notation of the power set by 2^A .
23. Some examples with ordered pairs:
 - (i) Consider the set of first names $P \triangleq \{Jacob, Moses, LittleRed, Frank\}$, and the set of last names $M \triangleq \{Jacob, RidingHood, Sinatra\}$. Then,

$$P \times M = \{(Jacob, Jacob), (Jacob, RidingHood), (Jacob, Sinatra),$$

$$(Moses, Jacob), (Moses, RidingHood), (Moses, Sinatra),$$

$$(LittleRed, Jacob), (LittleRed, RidingHood), (LittleRed, Sinatra),$$

$$(Frank, Jacob), (Frank, RidingHood), (Frank, Sinatra)\}.$$
 - (ii) Equality of pairs is sensitive to order, namely,

$$(Jacob, RidingHood) \neq (RidingHood, Jacob).$$
 - (iii) Obviously, $(Jacob, Jacob) = (Jacob, Jacob)$.
24. For every set X , $\emptyset \times X = \emptyset$.
25. For finite sets X and Y (regardless of their disjointness), $|X \times Y| = |X| \cdot |Y|$.
26. The Euclidean plane is the Cartesian product \mathbb{R}^2 . Every point in the plane has an x -coordinate and a y -coordinate. Thus a point p is a pair (p_x, p_y) . For example, the point $p = (1, 5)$ is the point whose x -coordinate equals 1 and whose y -coordinate equals 5.

1.2 Relations and Functions

9

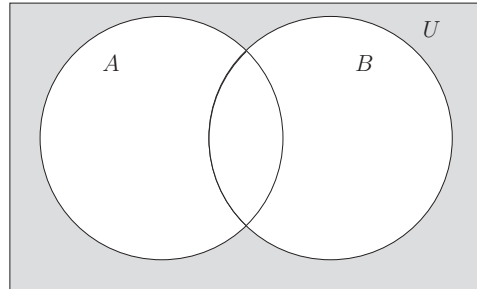


Figure 1.2. Venn diagram demonstrating the identity $U \setminus (A \cup B) = \bar{A} \cap \bar{B}$.

27. A circle C of radius r centered at the origin is the set of ordered pairs defined by $C \triangleq \{(x, y) \mid x^2 + y^2 = r^2\}$.
28. The Cartesian product of n identical sets $\{0, 1\}$ is denoted by $\{0, 1\}^n$, namely,

$$\{0, 1\}^n = \overbrace{\{0, 1\} \times \{0, 1\} \times \cdots \times \{0, 1\}}^{n \text{ times}}.$$

Every element in $\{0, 1\}^n$ is an n -tuple (b_1, \dots, b_n) , where $b_i \in \{0, 1\}$ for every $1 \leq i \leq n$. We refer to $b_i \in \{0, 1\}$ as a *bit* and to (b_1, \dots, b_n) as a *binary string*. We write a string without separating the bits by commas, for example, (i) 010 means $(0, 1, 0)$, (ii) $\{0, 1\}^2 = \{00, 01, 10, 11\}$, and (iii) $\{0, 1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

29. De Morgan's law states that $U \setminus (A \cup B) = \bar{A} \cap \bar{B}$. In Figure 1.2, a Venn diagram is used to depict this equality. A formal proof requires using propositional logic and is presented in Section 6.8.

1.2 RELATIONS AND FUNCTIONS

A set of ordered pairs is called a binary relation.

Definition 1.9 A subset $R \subseteq A \times B$ is called a *binary relation*.

A function is a binary relation with an additional property.

Definition 1.10 A binary relation $R \subseteq A \times B$ is a *function* if, for every $a \in A$, there exists a unique element $b \in B$ such that $(a, b) \in R$.

Figure 1.3 depicts a diagram of a binary relation $R \subseteq A \times B$. The sets A and B are depicted by the two oval shapes. The elements of these sets are depicted by solid circles. Pairs in the relation R are depicted by arcs joining the two elements in each pair. The relation depicted in Figure 1.3 is not a function because there are two distinct pairs in which the element $d \in A$ is the first element.

A function $R \subseteq A \times B$ is usually denoted by $R: A \rightarrow B$. The set A is called the *domain*, and the set B is called the *range*. Lowercase letters are usually used to denote functions, for example, $f: \mathbb{R} \rightarrow \mathbb{R}$ denotes a real function $f(x)$.

One can define new functions from old functions by using *composition*.

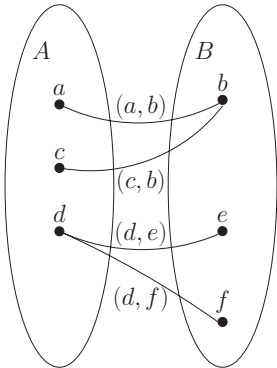


Figure 1.3. A diagram of a binary relation $R \subseteq A \times B$. The relation R equals the set $\{(a, b), (c, b), (d, e), (d, f)\}$.

Definition 1.11 Let $f : A \rightarrow B$ and $g : B \rightarrow C$ denote two functions. The *composed function* $g \circ f$ is the function $h : A \rightarrow C$ defined by $h(a) = g(f(a))$ for every $a \in A$.

Note that two functions can be composed only if the range of the first function is contained in the domain of the second function.

We can also define a function defined over a subset of a domain.

Lemma 1.1 Let $f : A \rightarrow B$ denote a function, and let $A' \subseteq A$. The relation R defined by $R \triangleq \{(a, b) \in A' \times B \mid f(a) = b\}$ is a function.

PROOF: All we need to prove is that for every $a \in A'$, there exists a unique $b \in B$ such that (a, b) is in the relation. Indeed, $(a, f(a)) \in R$, and this is the only pair in R whose first coordinate equals a . Namely, if both (a, b) and (a, b') are in the relation, then $f(a) = b$ and $f(a) = b'$, implying that $b = b'$, as required. ■

Lemma 1.1 justifies the following definition.

Definition 1.12 Let $f : A \rightarrow B$ denote a function, and let $A' \subseteq A$. The *restriction* of f to the domain A' is the function $f' : A' \rightarrow B$ defined by $f'(x) \triangleq f(x)$ for every $x \in A'$.

We denote *strict containment*, that is, $A \subseteq B$ and $A \neq B$, by $A \subsetneq B$. Given a function $f : A \rightarrow B$, we may want to extend it to a function $g : A' \rightarrow B'$, where $A \subsetneq A'$. This means that the relation f is a subset of the relation g .

Definition 1.13 A function g is an extension of a function f if f is a restriction of g .

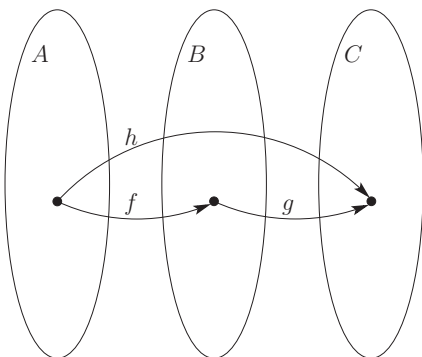


Figure 1.4. The functions $f : A \rightarrow B$ and $g : B \rightarrow C$ and the composed function $h : A \rightarrow C$ defined by $g \circ f$.