

**Part I**

**Propositional Logics**



# Chapter 1

## Introductory Concepts: Sets, Functions and Truth Functions

*Just by using mathematical methods, we can throw new and important light on the logical principles used in mathematics. This approach has led to more knowledge about logic in one century than had been obtained from the death of Aristotle up to 1847, when Boole's masterpiece was first published. –Oswald Spengler[90].*

*Students of mathematics are familiar with the phenomenon of “slow development,” or subconscious assimilation: the first time something new is studied the details seem too numerous and hopelessly confused, and no coherent impression of the whole is left on the mind. Then returning after a rest, it is found that everything has fallen into place with its proper emphasis –like the development of a photographic film. –E.T. Bell[9].*

*Mathematics rightly viewed possess not only truth, but supreme beauty—a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of painting or music, yet sublimely pure, and capable of a stern perfection such as only the greatest art can show. –Bertrand Russell[78].*

### 1.1 Logic: An Overview

#### 1.1.1 What is Logic For?

Formal logic is a branch of mathematics which was intended to describe and explain mathematical reasoning itself, and to provide a means by which to

understand what mathematics is about. In the western intellectual tradition, this question has deep connections with philosophy, and the quest to know the nature and structure of reality.

The modern search for an exact account of the logical principles of mathematical reasoning achieved its first notable success in the work of George Boole (1815 - 1864)[13]. The rules we are going to study include those of a special kind of algebra, **Boolean algebra**. In logic, we examine these rules and the mathematical structures which arise from them, as seen from the outside, so to speak, and we describe them mathematically.

But what is mathematics? It has been called many things: the language of science; the study of patterns; the science of calculation (partly true); the source of infallible truth and certainty (almost certainly false).

Euclid's *Elements of Geometry*[25] was long admired as the perfect realization of the ideal of certain knowledge: all of the results which had been discovered by the Athenian geometers, concerning plane figures, were shown to be the logical consequences of certain simple assumptions.

Ronald Reagan's bold assertion, that the Bible had to be divinely inspired, because it had been the best seller in the Western world for over two thousand years, should serve to support the case for a similar inspiration for the West's second best seller: Euclid's *Elements*.

But the notion that the Bible is an inerrant source of scientific truth, and Euclid's *Elements* an infallible source of mathematical truth were both discredited by the nineteenth century, in history by the higher criticism, in geology by strong evidence that the earth is far older than had been thought, in biology by a preponderance of evidence that biological species are not immutable, and in mathematics by the discovery of consistent alternatives to Euclid's geometry which in the last century have been shown to describe physical space.

Many before the start of the twentieth century confidently expected that the new science would supplant the old dogmas as a foundation for certainty immune to revision. Such hopes were roundly discredited in the first third of the twentieth century, both in natural science and in logic and mathematics as well.

But as the certainties of the past have been stripped of credibility, our scientific understanding of the physical world and the world of mathematics, while provisional, has exploded in recent times: more has been written and more has been learned in the past century or so than in all of human history. If ever there was or is a golden age of science and mathematics, it is now.

## 1.2 Sets

### The Most Frequently Encountered Concepts Involving Sets

An Overview: Intuitively, a **set** is a collection of things, and is something apart from its members. The sets we'll talk about are often

sets of logical formulas.<sup>1</sup> We use  $\Gamma$  and  $\Gamma'$  to refer to an arbitrary set of formulas, and  $X, Y, Z, \dots$  to refer to arbitrary formulas.  $\{X\}$  is the set consisting of the formula  $X$  alone, and is not the same as  $X$  itself. Similarly,  $\{X, Y\}$  is the set consisting of  $X$  and  $Y$  alone, and so on.

If  $A$  and  $B$  are sets (not necessarily sets of formulas),  $A \cap B$  (the **intersection**<sup>2</sup> of  $A$  and  $B$ ) is the set consisting of all those things which belong to both  $A$  and  $B$ . If  $A$  and  $B$  have no members in common, then  $A \cap B = \emptyset$ , where  $\emptyset$  is the **empty set**, or the set which has no members. On the other hand,  $A \cup B$  (the **union** of  $A$  and  $B$ ) is the set which consists of all those things that belong either to  $A$  or to  $B$  or to both. We generally write  $\Gamma, X$  instead of  $\Gamma \cup \{X\}$ , write  $\Gamma, X, Y$  instead of  $\Gamma \cup \{X, Y\}$ , and so on (but only when  $\Gamma$  is a set of formulas and  $X, Y, \dots$  are formulas).

We say that  $A$  is a **subset** of  $B$  and write  $A \subseteq B$  if every member of  $A$  is a member of  $B$ , and that  $A$  is a **proper subset** of  $B$  and write  $A \subset B$  if  $A$  is a subset of  $B$  but  $B$  is not a subset of  $A$ . The **power set** of  $A$ , or  $\mathbf{P}(A)$  is the set of all subsets of  $A$ .  $\emptyset$  is in  $\mathbf{P}(A)$ , since  $\emptyset$  is a subset of every set  $A$ , since there isn't any member of  $\emptyset$  which is not in  $A$  (because there isn't any member of  $\emptyset$ ). If  $A$  and  $B$  are subsets of each other then they are equal. This is the **principle of extensionality**.

### 1.2.1 Naming Sets

In the remainder of this chapter, we endeavor to provide an exact account of sets and functions, which we use throughout the text. Basically, a set is any collection of things, and a function is a rule for associating with any member of one set, a member of another. Both these concepts are important, because they are used extensively in mathematical logic to explain the underlying ideas. At a deeper level, many claim that *all* mathematical concepts can be defined in terms of sets, which then provide a "foundation" for mathematics, while others hold that all mathematical concepts can be defined in terms of functions.

Perhaps the best way of grasping these ideas is by using them, and so we recommend that to begin with, you do not spend too much time on this chapter, but return to it as needed to fill in the details.

In the remainder of this part we'll talk about sets. A **set** as we just said is a collection of things. The collection can have in it just about anything

---

<sup>1</sup>A logical formula, is the same as a formula in ordinary algebra which, like  $x \cdot (y + z)$ , is an expression which may appear on one side or the other of an equation. A logical formula is a formula of **Boolean** algebra, which we use in this book. The only difference is typographical: we use the capital letters 'A', 'B', 'C', ... instead of the lower case letters 'x', 'y', 'z', ... But we postpone an exact, rigorous definition of a logical formula (something rarely attempted in ordinary algebra) until Chapter 2.

<sup>2</sup>The symbols  $\cap, \cup, \in$  were introduced in 1889 by the Italian mathematician Giuseppe Peano (1858-1932).

you like. For example, there are nine major planets: Mercury, Venus, Earth, Mars, Jupiter, Saturn, Uranus, Neptune and Pluto<sup>3</sup>. These nine planets are the **members** or **elements** of the set of major planets. We also say that a set **contains** each of its members, and for any set  $A$ , we write ' $a \in A$ ' to mean ' $a$  is in  $A$ ', ' $a$  is an element of  $A$ ', ' $a$  is a member of  $A$ ' or ' $A$  contains  $a$ '.

One way of naming a set is to write down the names of each of its members in any order you like, using commas to separate each one from the other, and using braces or set brackets to enclose your list. This is a standard way of designating a set. For example, the set of major planets is,

$$\{Mercury, Venus, Earth, Mars, Jupiter, Saturn, Uranus, Neptune, Pluto\} .$$

But this is already getting a little awkward. Abbreviations would help. We could choose a letter as an abbreviation for each planet's name, making sure we don't use the same letter to **name** or **denote** different planets, and come up with an abbreviated list, such as,

$$\{m, v, e, r, j, s, u, n, p\}.$$

But even this can get out of hand, for example if you tried to use this notation, even in abbreviated form, to name the set of all people listed in the phone book. So another standard way of naming sets involves naming some defining property of the set. The set is the **extension** of its defining property. For example, the set of major planets is also the extension of the property of being a major planet, and we may write,

$$\{x : x \text{ is a major planet}\} . \tag{1.1}$$

Literally this means, "the set of all  $x$ , where  $x$  is a major planet".

We may go further: if we're talking about more than one set, we may decide to use letters to name the sets in question. For example, we might decide to let  $M$  be the set of major planets, and to let  $T$  be the set of terrestrial planets, the terrestrial planets being Mercury, Venus, Earth and Mars, in which case,  $M = \{m, v, e, r, j, s, u, n, p\}$ , while  $T = \{m, v, e, r\}$ .

### 1.2.2 The Principle of Extensionality: When are Two Sets Equal?

There are a number of ways of naming one and the same set. Two sets are equal **iff** (if and only if) they have the same members. In other words, two sets are equal **iff** neither set has a member which the other set lacks. This basic fact about sets is called the **principle (or the axiom) of extensionality** .

---

<sup>3</sup>Yes, we know. Pluto's status as a major planet is in question, but official recognition and common usage is unlikely to change any time soon, which is more a matter of history and politics than of astronomy.

So, for example, by the principle of extensionality,

$$\{x : x \text{ is a major planet}\} = \{m, v, e, r, j, s, u, n, p\} \quad (1.2)$$

$$= \{p, n, u, s, j, r, e, v, m\} \quad (1.3)$$

$$= \{m, m, v, e, r, j, s, u, n, p\}, \quad (1.4)$$

and so on. Observe that the order in which you name the planets, or even if in your list of planets you repeat the same name (such as in equation 1.4), you're still talking about the same set. By the principle of extensionality, all that matters is what's *in* the set, period.

### 1.2.3 Unit Sets, the Empty Set and Finite and Infinite Sets

A set might have only one member (we call them **unit sets** or **singleton sets**) or might even have no members at all. We call a set with no members **empty**. By extensionality, there can only be only one empty set, because by definition, no two empty sets can have a member which the other lacks. We are therefore justified in talking about *the* empty set ' $\emptyset$ '.

For example, here are two ways in which we might define the empty set,

$$\emptyset = \{x : x \neq x\}, \quad (1.5)$$

$$\emptyset = \{x : x \text{ is a unicorn}\}. \quad (1.6)$$

The first case would read literally "the set of all elements  $x$  which are not equal to themselves" (where  $\neq$  means 'is not equal to'). This set is empty because every  $x$  must be equal to itself. In the second case we have an empty set because unicorns do not exist.

The empty set has 0 members, any singleton set has 1 member, and in general, any **finite** set has  $n$  members, where  $n$  is a **natural number**, that is, a whole number which is either 0 or positive. A set which is not finite is **infinite**, and we say it has **infinitely many** members.

For instance, the set  $N$  of all natural numbers is infinite. It has more members than any natural number  $n$ , no matter how large, whether a billion, a billion billion, etc., because  $n + 1$  is a natural number even larger than  $n$ .

We may also write ' $\{0, 1, 2, \dots\}$ ' instead of ' $N$ ' to refer to the set of natural numbers. And we may write ' $\{3, 4, \dots, 10\}$ ' for the set of consecutive natural numbers starting with 3 and ending with 10. It is, of course, finite. The three dots after any comma mean 'and so on' whenever it's clear how to extend the list of items shown. In this case, the number after the comma is to exceed the number before the comma by 1.

### 1.2.4 Subsets, and Extensionality Again

When talking about sets in general, we use letters like ' $A$ ', ' $B$ ', ' $C$ ', and so on which may be any sets in some specified set of sets called the **domain** or

**universe of discourse**<sup>4</sup>. The letters are called **variables**, or in this case **set variables** to indicate that the universe consists of sets which the variables **vary over** or **range over**.

This enables us to state definitions and general rules. We may start with the definition of subsets: we define a set  $A$  to be a **subset** of  $B$  (and  $B$  to be a **superset** of  $A$ ) **iff** every member of  $A$  is a member of  $B$ , or more precisely,  $A$  has no member which  $B$  lacks. If  $A$  is a subset of  $B$ , we may write  $A \subseteq B$ . When  $A$  is a subset of  $B$ , we may also say that  $B$  **includes**  $A$ , that  $A$  **is included in**  $B$  or that  $B$  **contains**  $A$ <sup>5</sup>.

For example, if as before  $T$  is the set of terrestrial planets and  $M$  is the set of major planets, then  $T \subseteq M$ . On the other hand, if we let  $S$  consist of the terrestrial planets *and* their known natural satellites, then

$$S = \{Mercury, Venus, Earth, the moon, Mars, Phobos, Deimos\}, \quad (1.7)$$

and  $T$  is a subset of  $S$ , but  $S$  is *not* a subset of  $T$  or of  $M$ , because the satellites of Earth and Mars are neither terrestrial nor major planets.

By the definition of subsets, it follows that another way of stating the principle of extensionality is to say this:

**Principle of Extensionality:** If  $A$  and  $B$  are subsets of each other, then they are equal.

$A$  is **proper subset** of  $B$ , and we write  $A \subset B$  **iff**  $A$  is a subset of  $B$  but is not all of  $B$ . That is,  $A \subset B$  **iff**  $A \subseteq B$  and  $A \neq B$ . For example,  $T$  is a proper subset of  $M$ , but by definition is of course not a proper subset of itself.

We also assume, as a general rule, that a set is different from any of its members—it's not a member of itself.  $\{\text{the moon}\}$ , for example, is not the moon.  $\{\text{the moon}\}$  is an abstract object, a set which has one member, the moon, while the moon itself is a round mass of rock about a quarter of a million miles from the earth. By the same token,  $\{\{\text{the moon}\}\}$  is not  $\{\text{the moon}\}$ , for by extensionality,  $\{\{\text{the moon}\}\}$  has a single member, which is a set, while  $\{\text{the moon}\}$  does not contain a set, but rather a round rocky object which orbits the earth.

### 1.2.5 Basic Operations on Sets

The **intersection**  $A \cap B$  of  $A$  with  $B$  is the set of all those things which belong both to  $A$  and to  $B$ . We also say that  $A$  **meets**  $B$  **iff**  $A \cap B \neq \emptyset$ , and that  $A$  and  $B$  are **disjoint** **iff**  $A$  does not meet  $B$ , that is,  $A \cap B = \emptyset$ .

<sup>4</sup>The universe of discourse, or **universal set** must be a "well defined" set, and cannot contain everything. For instance, it cannot contain all sets which are not members of themselves. For as Bertrand Russell(1872-1970)[78] first pointed out, there cannot be a set  $M$  consisting of all sets that are not members of themselves, lest for every set  $x$ ,  $x \in M$  **iff**  $x \notin x$ , so that  $M \in M$  **iff**  $M \notin M$ , which is impossible.

<sup>5</sup>Yes, we know 'A contains e' also means that  $e$  is a member of  $A$ , while 'A contains B' means that  $A$  includes  $B$ ; unfortunately—and this is not uncommon when speaking informally even in mathematics—a word can have more than one meaning, and you have to decide which meaning is intended by the context, which works most of the time

The **union**  $A \cup B$  of  $A$  with  $B$  is the set of all things which belong either to  $A$  or to  $B$  (or to both), while the **complement** of  $A$  **relative** to  $B$ , or  $B - A$ , is the set of all those members of  $B$  which are *not* in  $A$ . We generally write  $-A$  for  $V - A$ , where  $V$  is the **universe of discourse**, and call it the **set complement** of  $A$ , or simply the **complement** of  $A$ , if the context is clear.

We may illustrate these definitions by means of **Euler diagrams**<sup>6</sup>. Suppose we represent the universe of discourse by a square: every member of the universe of discourse corresponds to a point inside the square. Inside the square, we draw a circle. Every member of  $A$  is to be represented by a point inside the circle, and non-members of  $A$  correspond to points in the square outside the circle, as shown in figure 1.1.

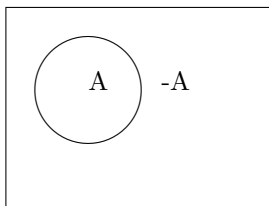


Figure 1.1: Euler Diagram

For union and intersection we need *two* circles, one representing  $A$  and one representing  $B$ . Then  $A \cap B$  will be the lens-shaped region where  $A$  and  $B$  overlap, while  $A \cup B$  will be the “binocular field” shape (at least the way it’s represented in cartoons) consisting of all points in  $A$  or in  $B$  or in both as shown in figure 1.2.

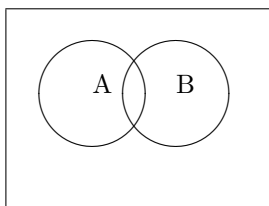


Figure 1.2: Intersecting Circles

The figure 1.2 divides the square into four regions, as labelled in figure 1.3.

The **power set**  $\mathbf{P}(A)$  of  $A$  is the set of *all* subsets of  $A$ , including  $A$  and the empty set. That is,  $\mathbf{P}(A) = \{B : B \subseteq A\}$ . For example, the two-element set  $\{0, 1\}$  has four subsets, because a given subset  $S$  can either contain or not

<sup>6</sup>The Swiss mathematician/physicist Leonard Euler (pronounced “oiler”) introduced his diagrams nearly 100 years before the more commonly known diagrams of British mathematician John Venn (1881). Venn diagrams are regimented. For instance, an Euler diagram depicting  $A \subseteq B$  puts the  $A$  circle inside the  $B$  circle, while a Venn diagram displays the same relation using the same diagram as Figure (1.2) except that the region  $A - B$  is shaded out, to indicate that it is empty or “uninhabited” ( $A - B$  is shown in Figure (1.3)).

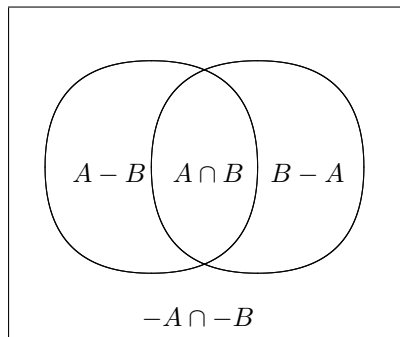


Figure 1.3: Four Regions

contain 0, and contain or not contain 1, making four possibilities in all as shown in the tree diagram of figure 1.4.

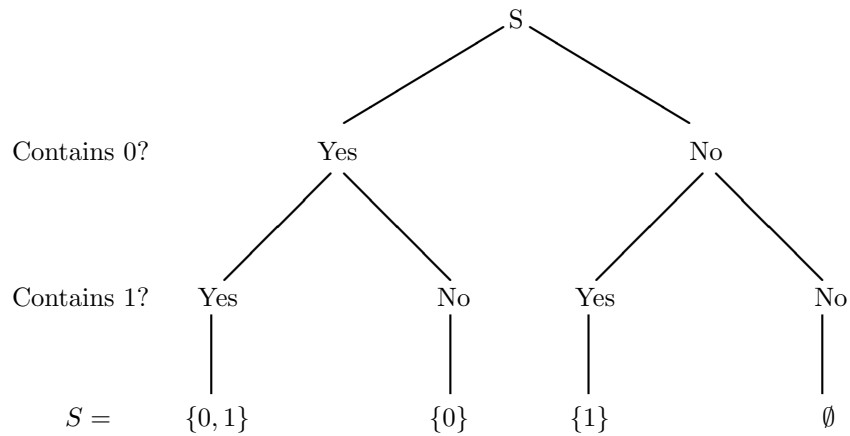


Figure 1.4: Tree Diagram

So the power set  $\mathbf{P}(\{0, 1\})$  of  $\{0, 1\}$  is the set,

$$\mathbf{P}(\{0, 1\}) \equiv \{\emptyset, \{0\}, \{1\}, \{0, 1\}\} . \tag{1.8}$$

In general, if  $A$  has  $n$  members, then  $\mathbf{P}(A)$  has  $2^n$  members. Let  $A$  be a *set of sets* (not necessarily finite). Then the **union**  $\cup A$  of a  $A$  is the set of all those

things which belong to at least one set in  $A$ . The **intersection**  $\cap A$  of  $A$  is the set of all those things which belong to all sets in  $A$ . For instance

$$\cup\{\{a, b\}, \{a, c\}, \{a, d\}\} = \{a, b, c, d\}, \quad (1.9)$$

$$\text{and } \cap\{\{a, b\}, \{a, c\}, \{a, d\}\} = \{a\}. \quad (1.10)$$

Another example: Let  $N^{>1}$  be the set of all natural numbers greater than 1 and let  $D_2 = \{4, 6, 8, \dots\}$  be the set of all numbers in  $N^{>1}$  which have 2 as a proper divisor. Similarly, let  $D_3 = \{6, 9, 12, \dots\}$  be the set of all numbers in  $N^{>1}$  with a proper divisor of 3, let  $D_4 = \{8, 12, 16, \dots\}$  and so on. Then the union of all such sets, namely  $\cup\{D_2, D_3, D_4, \dots\} = D_1 \cup D_2 \cup \dots$  is the set  $\{4, 6, 8, 9, 10, \dots\}$  of all numbers which have proper divisors in  $N^{>1}$ . These are the **composite numbers**.

**Prime numbers** are all numbers in  $N^{>1}$  which are not composite. The set of prime numbers is therefore the complement  $\{2, 3, 5, 7, 11, \dots\}$  of the set  $\cup\{D_2, D_3, D_4, \dots\}$  relative to  $N^{>1}$ . This is also the intersection,

$$\cap\{-D_2, -D_3, \dots\} = -D_2 \cap -D_3 \cap \dots, \quad (1.11)$$

of the set of complements of  $D_2, D_3, D_4, \dots$ . The ancient Greek mathematician Eratosthenes of Alexandria in the third century B.C.E. was the first to come up with a method for finding this intersection up to some given number, which has come to be known as the *sieve of Eratosthenes*.

First write out the natural numbers consecutively starting with 2 up to some number, say 24. Underline '2', which denotes the first number in the series, and then cross out every second number after that. Now underline the first number which has neither been underlined nor crossed out. This will be '3', so cross out every third number after that. When every number in the series has been either underlined or crossed out, the underlined numbers will be the prime numbers less than 24.

When you have underlined '3' and crossed out every third number after that, you may underline all the remaining numbers and there will be no more numbers to cross out. For since  $5 \cdot 5$  is greater than 24, any number less than 24 which is properly divisible by '5' must also be divisible by a prime number less than 5 and will already have been crossed out, and the same is true for all remaining primes less than 24. For instance, '10' and '20' have already been crossed out since both are in  $D_2$ , while '15' has been crossed out since it is in  $D_3$ , so that all numbers in  $D_5$  less than 24 have already been eliminated. The final result is:

$$\begin{array}{cccccccc} & \underline{2} & \underline{3} & \cancel{4} & \underline{5} & \cancel{6} & \underline{7} & \cancel{8} \\ \cancel{9} & \cancel{10} & \underline{11} & \cancel{12} & \underline{13} & \cancel{14} & \cancel{15} & \cancel{16} \\ \underline{17} & \cancel{18} & \underline{19} & \cancel{20} & \cancel{21} & \cancel{22} & \underline{23} & \cancel{24} \end{array}$$

## PROBLEMS

1. Call an *outer planet* a major planet which is not a terrestrial planet. Among the *Kuiper belt objects* or *KBO's* are Pluto and Varuna. What

is the intersection of the set of outer planets and the set of KBO's? Name the set by listing its elements, if any.

2. Name  $\mathbf{P}(\{1, 2, 3\})$  by listing its elements.
3. Call a *real number* a number which can be expressed in decimal form (where there may be infinitely many digits to the right of the decimal point), such as  $\pi$ , which to five decimal places is 3.14159. Call  $[0, 1/n]$  the set of all real numbers from 0 to  $1/n$  inclusive, where  $n$  is a non-zero natural number, and let  $\mathcal{R}$  be the set of real numbers. So

$$[0, 1/n] \equiv \{x \in \mathcal{R} : 0 \leq x \leq 1/n\} \text{ ,}$$

$$[0, 1/n] \equiv \{x \in \mathcal{R} : 0 \leq x \text{ and } x \leq 1/n\} \text{ .}$$

Also call  $(0, 1/n)$  the set of all real numbers between 0 and  $1/n$ , i.e.

$$(0, 1/n) = \{x \in \mathcal{R} : 0 < x < 1/n\} \text{ .}$$

Let  $P$  be the set of all sets of the form  $(0, 1/n)$  and let  $C$  be the set of all sets of the form  $[0, 1/n]$ .

- (a) What is  $\cap C$ ?
- (b) Is 0 in  $\cup P$ ?
- (c) What is  $\cap P$ ?
- (d) Let  $S$  be the set of all sets of the form,

$$[0, (n-1)/n] = \{x \in \mathcal{R} : 0 \leq x \leq (n-1)/n\}$$

Is 1 in  $\cup S$ ? Explain.

4. Show that to find all primes  $\leq n$  using the sieve method, you will already have crossed out all composite numbers when you have crossed out all of them with a factor  $\leq \sqrt{n}$ .

### 1.2.6 Ordered Pairs, Triples, Quadruples, etc.

A set  $\{a, b\}$  is sometimes called an **unordered pair**, because the order in which the members  $a$  and  $b$  are written doesn't matter. While the set  $\{a, b\}$  is an "unordered pair", which by extensionality is the same as  $\{b, a\}$ , the **ordered pair**  $\langle a, b \rangle$  consists of  $a$  and  $b$  *in that order*, and is **not** the same as  $\langle b, a \rangle$ , unless of course  $a = b$ . In fact, it can be shown that:

$$\begin{array}{ll} \text{If } \{a, b\} = \{c, d\}, & \text{then} \\ & \text{either } a = c \text{ and } b = d \\ & \text{or } a = d \text{ and } b = c . \end{array} \quad (1.12)$$

On the other hand, by definition of ordered pairs,

$$\text{If } \langle a, b \rangle = \langle c, d \rangle, \text{ then } a = c \text{ and } b = d . \quad (1.13)$$

Similarly, if  $\langle a, b, c \rangle$  and  $\langle d, e, f \rangle$  are **ordered triples**, and  $\langle a, b, c \rangle = \langle d, e, f \rangle$ , we require that  $a = d$ ,  $b = e$ , and  $c = f$ . And similar conditions apply to quadruples, quintuples, etc. Ordered pairs  $\langle a, b \rangle$ , ordered triples,  $\langle a, b, c \rangle$  and so on, are what we call **ordered  $n$ -tuples**: an ordered pair is a 2-tuple, a triple a 3-tuple, and so on. We sometimes write  $\mathbf{x}$  for the ordered  $n$ -tuple or “row vector”  $\langle x_1, x_2, \dots, x_n \rangle$ , and write  $\mathbf{a}$  for  $\langle a_1, a_2, \dots, a_n \rangle$ , and so on.

If  $A$  is any set, we write  $A^n$  for the set of all  $n$ -tuples of members of  $A$ . For instance,

$$\{0, 1\}^2 = \{\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 1, 0 \rangle, \langle 1, 1 \rangle\}, \quad (1.14)$$

and has four members, while  $\{0, 1\}^3$  has eight members:

$$\{\langle 0, 0, 0 \rangle, \langle 0, 0, 1 \rangle, \langle 0, 1, 0 \rangle, \langle 0, 1, 1 \rangle, \langle 1, 0, 0 \rangle, \langle 1, 1, 0 \rangle, \langle 1, 1, 1 \rangle\}. \quad (1.15)$$

By convention,  $\langle a \rangle = a$  and  $A^1 = A$ .

### 1.2.7 What Is an Ordered Pair?\*

Section Summary: There are many ways of defining ordered pairs, triples, etc. in terms of ordinary sets. We discuss Wiener’s definition, which is almost universally used.

As a matter of fact, we can define ordered pairs in terms of unordered pairs. The definition has to satisfy the condition (1.13). There are any number of definitions which satisfy (1.13), one of which, invented by Wiener[97], is in general use. Logicians and mathematicians don’t really care which definition is used, for as long as it satisfies (1.13), it does the same thing as any other definition that satisfies (1.13), and that’s all that matters.

By Wiener’s definition, the ordered pair  $\langle a, b \rangle$  is a set which contains two sets:  $\{a\}$  and  $\{a, b\}$ . By that definition,

$$\langle a, b \rangle = \{\{a\}, \{a, b\}\}. \quad (1.16)$$

Wiener’s definition does satisfy (1.13), for one can show,

$$\text{If } \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} \text{ then } a = c \text{ and } b = d. \quad (1.17)$$

Of course, like any other definition of ordered pairs along similar lines, Wiener’s definition *only* tells us when two ordered pairs, in the sense defined, are equal. It cannot by itself tell us which is the *first* and which the *second* element of a given pair. By convention, we take  $a$ , which is common to both members  $\{a\}$  and  $\{a, b\}$  of  $\{\{a\}, \{a, b\}\}$ , to be the first element, and  $b$  to be the last element, where  $b$  is not common to both  $\{a\}$  and  $\{a, b\}$ , unless of course  $a = b$ .

---

\*This part may be skipped without loss of continuity.

We also define an ordered triple to be an ordered pair, the first member of which is also an ordered pair: We define  $\langle a, b, c \rangle = \langle \langle a, b \rangle, c \rangle$ . Then

$$\langle a, b, c \rangle = \langle d, e, f \rangle, \quad (1.18)$$

$$\text{iff } \langle \langle a, b \rangle, c \rangle = \langle \langle d, e \rangle, f \rangle, \quad (1.19)$$

$$\text{iff } \langle a, b \rangle = \langle d, e \rangle \text{ and } c = f, \quad (1.20)$$

$$\text{iff } a = d \text{ and } b = e \text{ and } c = f. \quad (1.21)$$

In general then,

$$\langle a_1, a_2, \dots, a_{n-1}, a_n \rangle = \langle \langle a_1, a_2, \dots, a_{n-1} \rangle, a_n \rangle. \quad (1.22)$$

## 1.3 Functions

### Functions, Truth-Valued Functions and Truth Functions: An Overview of Sections 1.3 and 1.4

The formulas of Boolean logic stand for numbers, just as they do in ordinary algebra, except that the only numbers that they stand for have to be either 0 or 1, which we call **truth values**. A **function** is a rule which assigns to each member of some set  $D$ , its **domain**, a member of a set  $C$ , its **codomain**. The members of  $D$  are the **inputs** of the function, and the members of  $C$  are the **outputs**. A function may have more than one input. For instance, multiplication is a function which assigns to two numbers *in a given order*, the product of the two numbers, which is the output of the function.

The functions we most often come across are either **truth-valued functions**, the codomain of which is the set  $\{0, 1\}$  of truth values, or **truth functions**, which are truth-valued functions, the domain of which is the set of truth values, or the set of all pairs of truth values, or triples of truth values, and so on. A typical truth-valued function assigns a truth value to every formula in some set of formulas, while Boolean multiplication, which assigns to each pair of truth values their product, is an example of a truth function:  $1 \cdot 1 = 1$ ;  $1 \cdot 0 = 0 \cdot 1 = 0 \cdot 0 = 0$ .

Given a truth-valued function which assigns truth values to formulas, we call a formula in its domain **true** if the function assigns 1 to that formula, and we say that the formula is **false** if the function assigns 0 to it.

#### 1.3.1 On Functions

A **map** or **function** is any rule which assigns to each member of one set, called the **domain** (or **domain of definition**) of the function, one and only one member of a set we call the **codomain**. A function is a function **on** its domain  $D$ , and **maps  $D$  into** its codomain  $C$ , and is a function **from  $D$  to  $C$** .

Any member  $d$  of the domain of a function  $f$  (where the letter ‘ $f$ ’ is a **function symbol** which stands for  $f$ ) is an **input** of  $f$ . The **output**  $f(d)$  of  $f$  for a given input  $d$  is what  $f$  assigns to  $d$ . The term ‘ $f(d)$ ’ “makes sense” and  $f$

is **defined** at  $d$  only if  $d$  is in the domain of  $f$ . Put another way,  $f$  is **defined** on its domain, and is undefined elsewhere.

We write  $f : d \mapsto f(d)$  to say that  $f$  **sends** the element  $d$  of its domain to  $f(d)$ , and say that  $f(d)$  is the **value** of  $f$  **at** the input, **point** or **argument**  $d$ , or that  $f(d)$  is the **f-image** of  $d$ . For instance, if  $f : x \mapsto x^2$ ,  $f(x) = x^2$  for all  $x$  in  $D$ .

If  $A$  is a subset of the domain  $D$  of  $f$ , and  $B$  a subset of its codomain  $C$ , then the **f-image**  $f(A)$  of  $A$  is the set of all outputs of  $f$  whose inputs are in  $A$ . The **range** of  $f$  is  $f(D)$ , the  $f$  image of its domain. The **field** of  $f$  is the union  $D \cup f(D)$  of its domain and range. The **f-preimage**  $f^{-1}(B)$  of  $B$  is the set of all inputs of  $f$  whose outputs are in  $B$ . So,  $f(A) = \{f(x) : x \in A\}$  and  $f^{-1}(B) = \{x : f(x) \in B\}$ .

An **internal diagram** of a function displays its arrows, and members of the codomain and domain. As each member of the domain of  $f$  is assigned one and only one member of the codomain, each member of the domain is the source of exactly one arrow. The **graph** of a function  $f$  is the set of all **arrows**  $d \rightarrow f(d)$ , where  $d$  is an input of  $f$ . We say that  $d$  is the **source** and  $f(d)$  is the **target** of the arrow  $d \rightarrow f(d)$ .

In Fig. 1.5 below, for example, we display internal diagrams for five functions, call them  $m, u, k_1, c_1$  and  $i$ , each with the domain  $D = \{0, 1\}$ . The functions  $m, c_1$  and  $i$  have the same codomain as their domain  $D$ , while the codomain  $C$  of  $u$  is  $\{-1, 0, 1\}$ , and the codomain  $E$  of  $k_1$  is  $\{1\}$ .

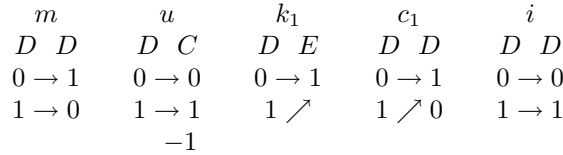


Figure 1.5: Internal Diagram for Five Functions

The function  $m$  is called the **Boolean complementation** function. The function  $i$  is called the **identity function**  $1_{\{0,1\}}$  on  $\{0, 1\}$ : its domain and codomain are equal, and it sends every element of its domain to itself. The function  $u$  is an **inclusion function** and has the same graph as  $i$  but is a different function because it has a different codomain. Again,  $k_1$  and  $c_1$  also have the same graphs, but are different functions. They are called **constant functions** because they have the same output no matter what the input.

Let  $f : D \rightarrow C$  and  $g : D_0 \rightarrow C_0$  be functions, where  $D_0 \subseteq D$  and  $C_0 \subseteq C$  and the graph of  $g$  is a subset of the graph of  $f$ , so that  $f(x) = g(x)$  for all  $x$  in  $D_0$ . Then we say that  $g$  is the **restriction** of  $f$  to  $D_0$  or is  $f$  **restricted** to  $D_0$  and we write  $g = f \mid D_0$ . We also say that  $f$  **extends**  $g$  or is an **extension** of  $g$ .

A function from  $D$  to  $C$  is **onto** or **maps  $D$  onto  $C$**  iff  $C$  is the range of  $f$ , so that each member of the codomain has been assigned to a member of the

domain (in the internal diagram, each member of codomain is the target of one or more arrows). In the above example, the functions  $m, k_1$  and  $i$  map their common domain  $\{0, 1\}$  onto their respective codomains.

A function  $f$  is **one-to-one** or maps its domain **one-to-one** into its codomain **iff** every point in the codomain is the target of no more than one arrow in the internal diagram of  $f$ . The functions  $m, u$  and  $i$  in the above example map their common domain  $\{0, 1\}$  one-to-one into their respective codomains.

The functions  $m$  and  $i$  are both one-to-one and onto, and map their domains one-to-one onto their codomains;  $u$  maps  $\{0, 1\}$  one-to-one into its codomain  $\{-1, 0, 1\}$  but not onto it;  $k_1$  maps its domain  $\{0, 1\}$  onto its codomain, but is not one-to-one, while  $c_1$  neither maps its domain one-to-one nor onto its codomain. A function which maps a set  $A$  one-to-one onto  $B$  is called a **one-to-one correspondence** from  $A$  and  $B$ . If there is a one-to-one correspondence  $f$  from  $A$  to  $B$ , there is also a one-to-one correspondence  $f^{-1}$  from  $B$  to  $A$ . The internal diagram of the **inverse**  $f^{-1}$  of  $f$  is just the internal diagram of  $f$  with the arrows reversed.  $f$  and  $f^{-1}$  are both one-to-one correspondences **between**  $A$  and  $B$ . A one-to-one correspondence from  $A$  to itself is a **permutation** of  $A$ . To summarize:

	$m$	$u$	$k_1$	$c_1$	$i$
	$D \ D$	$D \ C$	$D \ E$	$D \ D$	$D \ D$
	$0 \rightarrow 1$	$0 \rightarrow 0$	$0 \rightarrow 1$	$0 \rightarrow 1$	$0 \rightarrow 0$
	$1 \rightarrow 0$	$1 \rightarrow 1$	$1 \nearrow$	$1 \nearrow 0$	$1 \rightarrow 1$
		-1			
<i>Onto?</i>	<i>Yes</i>	<i>No</i>	<i>Yes</i>	<i>No</i>	<i>Yes</i>
$1 - 1?$	<i>Yes</i>	<i>Yes</i>	<i>No</i>	<i>No</i>	<i>Yes</i>
$1 - 1 \text{ Corr?}$	<i>Yes</i>	<i>No</i>	<i>No</i>	<i>No</i>	<i>Yes</i>

Figure 1.6: Maps

We say that two sets  $A$  and  $B$ , whether finite or infinite, have the **same number of members** or that  $A$  and  $B$  are **equinumerous**, or that  $A$  **has as many members** as  $B$  **iff** there is a one-to-one correspondence between  $A$  and  $B$ . We also say that  $B$  has **more** members than  $A$  if no function maps  $A$  onto  $B$ .

In terms of functions, we may define a set  $A$  to be **finite** **iff** either  $A$  is empty, in which case it has zero members, or has as many members as a set  $\{1, 2, \dots, n\}$  of consecutive positive integers or natural numbers starting with 1 and ending with  $n$ . We then say that  $A$  has  $n$  members. If  $A$  is not finite, it is **infinite**.

No finite set is equinumerous with some proper subset of itself, but every infinite set is. For instance, the set  $N$  of natural numbers is equinumerous with the set  $E$  of even natural numbers, since the function  $e$  from  $N$  to  $E$  defined by the condition  $e(n) = 2n$  is a one-to-one correspondence from  $N$  to  $E$  with the internal diagram in figure 1.7.

This gives us an alternative definition of finite sets: a set is **finite** **iff** it is

$$\begin{array}{rcl}
 e : N & \longrightarrow & E \\
 0 & \longrightarrow & 0 \\
 1 & \longrightarrow & 2 \\
 2 & \longrightarrow & 4 \\
 3 & \longrightarrow & 6 \\
 & & \vdots
 \end{array}$$

Figure 1.7: Natural Number Equinumerous with Even Natural Numbers

not equinumerous to any proper subset of itself, and is **infinite** otherwise<sup>7</sup>.

A set which is equinumerous to  $N$  is **denumerable**, while a **countable** set is a set which is equinumerous to some subset of  $N$ , and so is either finite or denumerable. A denumerable set is thus countably infinite.

A set is **uncountable iff** it's not countable. As Georg Cantor(1845-1918) showed[17], the set of fractions  $m/n$ , where  $m$  and  $n$  are positive integers is denumerable<sup>8</sup>. He also showed, as we'll see in Chapter 8, that  $\mathbf{P}(N)$  is uncountable.

If  $f$  is a function which maps  $D$  into  $C$ , we may write  $f : D \longrightarrow C$  or  $D \xrightarrow{f} C$ . Either of these figures is called an **external diagram** for  $f$  and

---

<sup>7</sup>Here's one way to illustrate these ideas: "Hilbert's Hotel"[36], widely renowned but not to be confused with the Hilton, whose rooms can be sold out, has infinitely many rooms, numbered 1, 2, 3, ... Suppose that the hotel is full - every room is occupied, when a traveler comes in asking for a room. "No problem", says the clerk at the front desk, and she moves the occupants of Room 1 into Room 2, the occupants of Room 2 into room 3, and so on all along the line, leaving Room 1 available to the traveller. Next, suppose that the hotel is full, and a denumerable number of travellers come in asking for rooms. "No problem", the desk clerk repeats, and moves the occupants of Room 1 into Room 2, the occupants of Room 2 into Room 4, the occupants of Room 3 into Room 6, and so on. This leaves all the odd numbered rooms unoccupied, and available for the waiting travellers

<sup>8</sup>Since the members of the set of positive fractions can be listed in sequence, it is countable. Start with 1/1, the only positive fraction such that the sum of the numerator and denominator is 2. There are two for which this sum is 3 : 1/2 and 2/1, three for which the sum is 4 : 1/3, 2/2, 3/1, etc. So the first six fractions of the sequence are:

$$\begin{array}{cccccc}
 1 & 2 & 3 & 4 & 5 & 6 \\
 1/1 & 1/2 & 2/1 & 1/3 & 2/2 & 3/1
 \end{array}$$

and we have a one-to-one correspondence  $c : N^+ \longrightarrow Fr^+$  between the set  $N^+$  of positive natural numbers and  $Fr^+$ . Since there can be no more positive rational numbers than there are fractions, and also no more positive natural numbers than there are positive rational numbers, and  $N^+$  is infinite, the set of positive rational numbers must be denumerable.

may be used to denote  $f$  or to assert that  $f$  maps  $D$  into  $C$ <sup>9</sup>. The context will determine which of these usages is intended. The external diagrams for the functions  $m, u, k_1, c_1$  and  $i$  are:

$$\begin{array}{llll}
 m : \{0, 1\} & \longrightarrow & \{0, 1\} & & m : D & \longrightarrow & D \\
 u : \{0, 1\} & \longrightarrow & \{-1, 0, 1\} & & u : D & \longrightarrow & C \\
 k_1 : \{0, 1\} & \longrightarrow & \{1\} & \text{ or more concisely: } & k_1 : D & \longrightarrow & E \\
 c_1 : \{0, 1\} & \longrightarrow & \{0, 1\} & & c_1 : D & \longrightarrow & D \\
 i : \{0, 1\} & \longrightarrow & \{0, 1\} & & i : D & \longrightarrow & D
 \end{array}$$

A function  $\sigma$ , which maps the set  $S_n = \{1, \dots, n\}$  into a set  $A$  is called a **finite sequence** of elements of  $A$  **indexed** by  $S_n$ , and is generally written as  $\sigma_1, \dots, \sigma_n$  where  $\sigma_1$  is  $\sigma(1)$ ,  $\sigma_2$  is  $\sigma(2)$  and so on up to  $\sigma_n = \sigma(n)$ . Each arrow  $i \longrightarrow \sigma(i)$  (where  $i \in \{1, \dots, n\}$ ) is an **occurrence** of the **term**  $\sigma_i$  in the sequence  $\sigma$ . If  $\sigma$  maps  $N^+$ , the set of non-zero natural numbers, into  $A$ , then  $\sigma$  is an **infinite sequence indexed** by  $N^+$ , which is generally written as  $\sigma_1, \sigma_2, \dots$ .

If  $f : B \rightarrow C$  and  $g : A \rightarrow B$ , so that the codomain of  $g$  is the domain of  $f$ , we say that the **composition**  $f \circ g$  or  $fg$  of  $f$  with  $g$  is the function  $fg : A \rightarrow C$  defined by the condition  $(fg)(x) = f(g(x))$  for all  $x$  in  $A$ . The composition of  $f$  with  $g$  is **defined iff** the codomain of  $g$  is the domain of  $f$ .

If in addition we have  $h : C \rightarrow D$ , then  $hf : B \rightarrow D$  is also defined, for  $(hf)(y) = h(f(y))$ , for all  $y$  in  $B$ . Then both  $(hf)g : A \rightarrow D$  and  $h(fg) : A \rightarrow D$  are likewise defined. Moreover,  $h(f(g(x))) = h((fg)(x)) = (h(fg))(x)$  and  $h(f(g(x))) = (hf)(g(x)) = ((hf)g)(x)$ , for all  $x$  in  $A$ , so that  $h(fg) = (hf)g$ . We say that composition is **associative** whenever it is defined.

You can find the composition of two functions by combining their internal diagrams. For instance, let  $c_0(0) = c_0(1) = 0$ , where  $c_0 : \{0, 1\} \rightarrow \{0, 1\}$ . To find the composition  $mc_0$ , just follow the arrows in the composite diagram on the left, the middle column of which is both the codomain of  $c_0$  and the domain of  $m$ , to get the internal diagram for the composition on the right:

Note  $fg$  need not be same as  $gf$ . For instance,  $c_0m = c_0$ , but  $mc_0 = c_1$ . We express this fact by saying that composition is not necessarily **commutative** and that as this particular example shows,  $c_0$  and  $m$  do not **commute** with each other.

If  $f : A \rightarrow B$  and  $g : B \rightarrow A$ , then  $fg$  and  $gf$  are both defined, and if  $fg = \mathbf{1}_B$ , we say that  $f$  is a **left inverse** of  $g$ , and  $g$  is a **right inverse** of  $f$ . The following facts are useful:

---

<sup>9</sup>We may take an arrow  $D \xrightarrow{f} C$ , which is the external diagram for the function  $f$ , to be a triple  $\langle D, f, c \rangle$ , where ‘ $f$ ’ “labels” the arrow  $D \rightarrow C$ . Arrows with different labels may thus have both the same source and the same target. Then the external diagram of a function  $f$  may be identified with such an arrow. But by definition, no two arrows in the internal diagram of a function, may have the same source. So we may identify an arrow of the internal diagram of a function with an ordered pair, the first member of which is the source and the second the target of the arrow. It is usual for set theorists, but not algebraists, to identify a function with its graph, which is then taken to be a set of ordered pairs. (Of course, an  $n$ -ary function is then identified with a set of  $n+1$ -tuples, each of which is an ordered pair, the first member of which is an  $n$ -tuple of inputs).

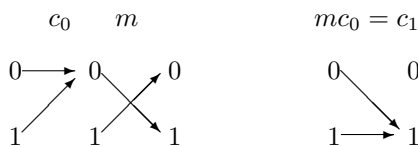


Figure 1.8: Composition

- $f$  maps  $A$  onto  $B$  iff it has a right inverse  $g$ <sup>10</sup>
- $g$  maps  $B$  one-to-one into  $A$  iff it has a left inverse  $f$ <sup>11</sup>

## PROBLEMS

### 1. Internal Diagrams

- Provide an internal diagram for both of the left inverses of  $u$ .
- Provide an internal diagram for both of the right inverses of  $k_1$ .

### 2. Permutations

- Let a permutation  $p$  of  $A$  be an **involution** iff  $pp = \mathbf{1}_A$ . Show that both permutations of  $\{0, 1\}$  are involutions.
- Find an involution of  $\{1, 2, 3\}$ .
- Find a permutation of  $\{1, 2, 3\}$  which is not an involution.
- Find two distinct permutations of  $\{1, 2, 3\}$ , neither of which is the identity permutation  $\mathbf{1}_{1,2,3}$ , which commute with each other.
- Find two permutations of  $\{1, 2, 3\}$  which do not commute with each other.

<sup>10</sup>For if  $f : A \rightarrow B$  has a right inverse  $g : B \rightarrow A$ ,  $f$  must be onto, so that the domain of  $g$  is indeed  $B$ . And if  $f$  is in fact onto, we may construct a right inverse, since each point in  $B$  is a target of at least one arrow in the graph of  $f$ . Choose one such arrow and reverse it, and do the same thing for every other point in  $B$ . Then the set of all the arrows thus obtained is the graph of a right inverse of  $f$ .

<sup>11</sup>If  $g$  has a left inverse  $f : A \rightarrow B$ , then  $g$  is one-to-one. For suppose that  $b_1$  and  $b_2$  are points in  $B$  such that  $g(b_1) = g(b_2)$ . Then  $f(g(b_1)) = f(g(b_2))$ . But  $f(g(b_1)) = b_1$  and  $f(g(b_2)) = b_2$  so  $b_1 = b_2$ . On the other hand, if  $g$  is one-to-one, reverse all the arrows in its graph. The set of all such arrows will then be a subgraph of a left inverse  $f : A \rightarrow B$  of  $g$ , but may not be defined at all points in  $A$ . For each such undefined point  $a$ , let  $f$  send  $a$  to an arbitrary point in  $B$ . Then  $f$  is indeed a left inverse of  $g$ .

If  $f : A \rightarrow B$  has both a right inverse  $g_2 : B \rightarrow A$ , so that  $fg_2 = \mathbf{1}_B$  and a left inverse  $g_1 : B \rightarrow A$ , so that  $g_1f = \mathbf{1}_A$ , then  $g_1 = g_2$ . For  $g_1 = g_1\mathbf{1}_B = g_1(fg_2) = (g_1f)g_2 = \mathbf{1}_A g_2 = g_2$ . Thus if  $g$  has both a left inverse and a right inverse, it also has a **two-sided inverse**, which is both a left and a right inverse. So  $f$  has at most one two-sided inverse  $f^{-1}$ , for if  $g_1$  and  $g_2$  are two-sided inverses of  $f$ ,  $g_1$  is also a left inverse and  $g_2$  a right inverse of  $f$ , so  $g_1 = g_2$ .

### 1.3.2 Functions with Several Inputs

A function may also have more than one input. For example, when you add two numbers, the two numbers you added are the inputs, and their sum is the output. We call a function  $f$  with  $n$  inputs ( $n = 1, 2, \dots$ ) an  **$n$ -ary function**, and call  $n$  the **arity** of  $f$ . Functions are sometimes called **operations**, a term most commonly used for **binary** or **2-ary functions**.

For example, we might write ' $p(x, y)$ ' for  $x$  plus  $y$ . Although we arbitrarily chose the letter ' $p$ ' to represent addition, it's much more common to refer to the sum of  $x$  and  $y$  by putting a plus sign between the ' $x$ ' and the ' $y$ '. So by our definition,  $p(x, y) = x + y$ . For example,  $p(2, 3) = 5$ . The term ' $p(x, y)$ ' gives the sum of  $x$  and  $y$  in "functional notation," while ' $x + y$ ' gives it in "algebraic" or "operator" notation, which is used only for binary function symbols like the addition and multiplication signs.

In a similar spirit, we might write ' $t(x, y)$ ' for  $x$  times  $y$ , instead of putting a multiplication sign between the ' $x$ ' and the ' $y$ '; this can be either ' $\times$ ', ' $\cdot$ ' or no sign at all. So we may write ' $t(x, y) = x \cdot y$ ', ' $t(x, y) = x \times y$ ' or even ' $t(x, y) = xy$ '. It's also common to put an arabic numeral in place of the first factor  $x$  of  $xy$ , but not for the second factor  $y$ . We may write ' $2y$ ' for ' $2 \cdot y$ ', for example, but we can't also put, say, ' $3$ ' for ' $y$ ', for  $2 \times 3$  is 6, not 23.

In the case of addition and multiplication, the order of the inputs doesn't matter, because no matter what numbers  $x$  and  $y$  you choose,  $x + y$  is always the same as  $y + x$  and  $x \cdot y$  is always the same as  $y \cdot x$ . Addition and multiplication of numbers is said to be **commutative**. On the other hand, subtraction is not commutative. For example,  $2 - 1 = 1$ , while  $1 - 2 = -1$ . And neither is division: for example,  $2/1$  is 2, which is different from  $1/2$ .

It's often useful in logic to treat *all* functions as if they have only one input. One way of doing this for a function with two inputs is to replace the two inputs  $x$  and  $y$  with a *single entity*: the ordered pair  $\langle x, y \rangle$ . Then, for example, the function  $p$  defined above, which assigns to any two inputs  $x$  and  $y$  their sum, now sends the **ordered pair**  $\langle x, y \rangle$  to  $x + y$ , and if its inputs are all positive integers or nonzero natural numbers, its domain is now the set  $P^2$  of all *ordered pairs* of positive integers, while its codomain might be the set  $P$  of all positive integers. Then  $p(x, y)$  is really  $p(\langle x, y \rangle)$ , even though we will conform to the common practice and always write  $p(x, y)$ .

Similarly, we may take a function with three inputs  $x$ ,  $y$  and  $z$  in that order to be a function with a single input  $\langle x, y, z \rangle$ . And so on for functions with more than three inputs.

We may also form compositions of functions of several inputs with other functions. Their values are best specified by formulas. For instance, suppose that  $f : P^2 \rightarrow P$  is a composition of addition and multiplication of positive integers, defined by the condition that,

$$f(x, y) = (x + y) + xy. \quad (1.23)$$

The formula on the right side of this equation specifies what the output of  $f$  is, for given inputs  $x$  and  $y$ , and thus determines each arrow of the internal

diagram for  $f$ . For example, one of these will be,

$$\langle 2, 3 \rangle \mapsto 11, \quad (1.24)$$

since  $2 + 3 + (2 \cdot 3) = 11$ .

When the domain and codomain of  $f$  are given, the function  $f$  defined by the condition (1.23) is the function **determined** by the formula  $(x + y) + xy$  (where the variables in alphabetical order correspond to the order of the inputs of  $f$ ).  $f$  is then  $f : \langle x, y \rangle \mapsto (x + y) + xy$ , and for  $f$  we may simply write  $\langle x, y \rangle \mapsto (x + y) + xy$ .

## PROBLEMS

1. Let logical complementation  $- : \{0, 1\} \longrightarrow \{0, 1\}$  be defined by the condition that  $-A = 1$  if  $A = 0$  and  $-A = 0$  if  $A = 1$ . The negation  $-$  is therefore the function from  $\{0, 1\}$  to  $\{0, 1\}$  determined by ‘ $-A$ ’. Also let  $+ : \{0, 1\}^2 \longrightarrow \{0, 1\}$  be defined by the condition that  $A + B = 1$  if  $A \neq B$  and  $A + B = 0$  if  $A = B$ . Provide an internal diagram for the function determined by the formula ‘ $-(A + B)$ ’.

## 1.4 Truth Functions

### 1.4.1 Truth Valued Functions and Truth Functions

One of the most important questions in logic is whether one statement  $\Phi$  is a **logical consequence** of another statement  $\Sigma$ . Here  $\Sigma$  and  $\Phi$  are arbitrary statements. The idea is that  $\Phi$  is a logical consequence of  $\Sigma$  **iff** it’s not possible or even conceivable that  $\Sigma$  is true and  $\Phi$  is false.

For instance, if  $\Sigma$  is “the earth is flat and the north star is 3,000 miles above the north pole” and  $\Phi$  is “the earth is flat,” then  $\Phi$  is a logical consequence of  $\Sigma$ .

Observe that the question of whether or not  $\Sigma$  is true is irrelevant to the question of whether  $\Phi$  is a logical consequence of  $\Sigma$ . You don’t have to know whether  $\Sigma$  is true or not to know that  $\Phi$  is a logical consequence of  $\Sigma$ . But what in this example does it mean to say that a statement  $\Sigma$  is true? Aristotle’s answer is good enough for mathematical and scientific purposes. In our modern terminology, suppose  $\Sigma$  is the statement “the earth is round”. Then  $\Sigma$  is true **iff** the earth is round. More directly, “the earth is round” is **true iff** the earth is round.

Note that  $\Sigma$  is true whether you believe it or not. When people believed that the earth is flat, that popular belief didn’t make it true, nor did the earth change its shape and become round when people began believing that it was round.

In Boolean logic, we approach the problem of logical consequence by using the concept of function. It is convenient to assign the number 1 to any true

statement, and the number 0 to any false statement: 1 is the **truth value** of any true statement and 0 is the **truth value** of any false statement.

A function, the codomain of which is the set  $\{0, 1\}$ , is a **truth valued function**. For instance, the function  $f : S \rightarrow \{0, 1\}$ , that assigns each member of some given set  $S$  of statements a truth value, is a truth valued function. The **cokernel**  $\text{cok}(f)$  of  $f$  is then the set  $f^{-1}(\{1\})$  of all true statements in  $S$ .

A truth valued function, the domain of which is  $\{0, 1\}^n$  ( $n = 1, 2, \dots$ ) is a **truth function**. For instance, there are four 1-ary truth functions, since the input 0 can have one of two outputs and so can the input 1. As we have seen, the 1-ary truth functions are  $m, c_0, c_1$  and  $i$ . There are four input pairs for a 2-ary truth function, and two possible outputs for each pair, giving sixteen 2-ary truth functions. And so on.

Of the sixteen binary truth functions, the Boolean operations:

- logical complementation
- $\vee$  logical addition<sup>12</sup>
- $\wedge$  logical multiplication

are special, for the identities  $BA$  below define the rules of Boolean algebra in a natural way. We'll write:  $\neg A$  for the **Boolean complement**  $m(A)$  of  $A$ , while Boole[13] wrote:  $1 - A$ , which coincides with the ordinary *arithmetical* value when  $A$  is a truth value. We also write  $A \wedge B$  while Boole[13] wrote  $AB$ , the arithmetical value, and we write  $A \vee B$  instead of Boole's  $A + B$ , which is the same as the arithmetical value when  $A$  and  $B$  are truth values, except that  $1 \vee 1$  is 1, not 2.

An important sort of truth valued function is the **characteristic function** of a set. Let  $V$  be a non-empty set, let  $A$  and  $B$  be subsets of  $V$ , and  $x$  and  $y$  be elements of  $V$ . Then the characteristic function  $c_A : U \rightarrow \{0, 1\}$ , is defined thus:

$$c_A(x) \equiv \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A \text{ (i.e. } x \text{ is not in } A) . \end{cases} \quad (1.25)$$

We see that  $c_A(x)$  is therefore the truth value of ' $x \in A$ '. Note that,

$$c_{\neg A}(x) = \neg c_A(x) , \quad (1.26)$$

where  $\neg A \equiv V - A$ , the complement of the set  $A$  (relative to  $V$ ). Also,

$$c_{A \cap B}(x) = c_A(x) \wedge c_B(x) , \quad (1.27)$$

$$c_{A \cup B}(x) = c_A(x) \vee c_B(x) . \quad (1.28)$$

Observe too that to every truth valued function  $f$  on  $V$ , there corresponds a unique set  $\text{cok}(f)$ , whose characteristic function is  $f$ , and that for every subset  $A$  of  $V$ , there is a unique truth valued function  $c_A$ , whose cokernel is  $A$ . Thus there is a one-to-one correspondence between subsets of  $V$  and their characteristic

<sup>12</sup>The symbol for logical addition  $\vee$  comes from the Latin letter 'v' which stands for the Latin word 'vel', which means 'or' in the inclusive sense.

functions. This allows us later on to identify a property  $R$  either with the extension of  $R$ , or with the characteristic function of the extension of  $R$ .

One example of a 3-ary truth function is the function  $t : \{0, 1\}^3 \rightarrow \{0, 1\}$  determined by the formula ‘ $A \wedge (B \wedge C)$ ’. We call the letters ‘ $A$ ’, ‘ $B$ ’ and ‘ $C$ ’ in this formula, which are themselves formulas, **propositional variables**, or more specifically, **Boolean variables**. The formulas ‘1’ and ‘0’ always denote the truth values 1 and 0, and are **propositional constants**, or more specifically, **Boolean constants**.

Boolean variables **range over** a set  $D$ . It is the domain of the **logical complementation function**  $- : D \rightarrow D$  while  $D^2$  is the domain of the Boolean multiplication and addition operations  $\wedge : D^2 \rightarrow D$  and  $\vee : D^2 \rightarrow D$  provided that the following equations are **identities**, they hold for all  $A, B$  and  $C$  in  $D$ :

$$\begin{array}{lll}
 \text{Commutativity} & A \wedge B = B \wedge A & \\
 & A \vee B = B \vee A & \\
 \\
 \text{Associativity} & A \wedge (B \wedge C) = (A \wedge B) \wedge C & \\
 & A \vee (B \vee C) = (A \vee B) \vee C & \\
 \\
 \text{Distributivity} & A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C) & (1.29) \\
 & A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C) & \\
 \\
 \text{Identity} & A \wedge 1 = A & A \vee 0 = A \\
 \text{Absorption}^{13} & A \vee 1 = 1 & A \wedge 0 = 0 \\
 \text{Complementation} & A \wedge -A = 0 & A \vee -A = 1
 \end{array}$$

The set  $D$ , which contains distinct elements 0 and 1, taken together with the **unary function**  $- : D \rightarrow D$  and the binary functions  $\wedge : D^2 \rightarrow D$  and  $\vee : D^2 \rightarrow D$ , constitute a **Boolean algebra**, provided that the functions  $-$ ,  $\wedge$  and  $\vee$  obey the identities eq. (1.29) above. Thus we distinguish between a Boolean algebra taken as an entity, and “Boolean algebra” taken as a subject, namely the study of Boolean algebras.

Boole[13] recognized that his rules hold when the **domain of discourse**  $D$  is the power set of a set  $V$ , the **universe** of discourse, and  $-$  becomes set complementation (relative to  $V$ ), while  $\wedge$  and  $\vee$  become the set intersection operation  $\cap : D^2 \rightarrow D$  and the set union operation  $\cup : D^2 \rightarrow D$  respectively, 0 becomes  $\emptyset$  and 1 becomes  $V$ . If  $V = \{\emptyset\}$ , then  $0 = \emptyset$  and  $1 = \{\emptyset\}$ , and operators:  $-$ ,  $\cap$ ,  $\cup$  become the truth functions:  $-$ ,  $\wedge$ ,  $\vee$ .

---

<sup>13</sup>These rules are special cases of the absorption laws:  $A \wedge (A \vee B) = A$  and  $A \vee (A \wedge B) = A$

We shall be concerned mainly with Boole's second interpretation, the **two-element Boolean algebra**  $\mathbf{B}_2$ , the domain of which is  $\mathbf{P}(\emptyset) = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$  (which is often written as ' $\mathbf{2}$ ' in the literature<sup>14</sup>). **Boolean logic** is the study of the  $\mathbf{B}_2$ . There is more to  $\mathbf{B}_2$  than meets the eye, as we shall see in the next three chapters and in section 8.5.6 (page 161).

## PROBLEMS

1. Provide an internal diagram for the characteristic function of the subset  $\{0\}$  of  $\{0, 1\}$ . It is the internal diagram for a truth function, which was displayed in section 1.3.1, figure 1.6 (page 16), together with those of other functions. Which one of them is it? Is it the same as the function defined in the problem at the end of the previous section (page 21).
2. Internal Diagrams
  - (a) Provide internal diagrams for the characteristic functions of the following subsets of  $\{0, 1\}^2$ :
 
$$\{\langle 1, 1 \rangle\}$$

$$\{\langle 1, 1 \rangle, \langle 1, 0 \rangle, \langle 0, 1 \rangle\}$$
  - (b) Provide an internal diagram for the characteristic function of the subset  $\{1\}$  of  $\{0, 1\}$ .
3. Find the sets, the characteristic functions of which are the truth functions  $\neg, \wedge, \vee$  respectively. (Hint: find the cokernels of these truth functions).
4. How many function are there from  $\{0, 1\}^3$  to  $\{0, 1\}$ ?

---

<sup>14</sup>By Von Neumann's well known definition of natural numbers in terms of sets (also mentioned in section 8.4.4 page 161),

$$\begin{aligned} 0 &= \emptyset, \\ 1 &= \{\emptyset\} = 0 \cup \{0\} = \{0\}, \\ 2 &= \{\emptyset, \{\emptyset\}\} = 1 \cup \{1\} = \{0, 1\} \\ &\vdots \end{aligned}$$

Thus the universe of discourse  $\{0, 1\}$  of the two-element Boolean algebra  $\mathbf{B}_2$  may also be taken to consist of sets, namely the two sets  $\emptyset$  and  $\{\emptyset\}$ . This is why the set  $\{0, 1\}$  is often written as ' $\mathbf{2}$ ' in the literature.