CHAPTER 5

Sets and relations

5.1 Sets

In this chapter, we will present some basic mathematical ideas about sets and relations. Some of the material on sets may be familiar to you already, in which case you may wish to scan over those sections fairly briefly. The main reason for introducing sets is to provide some useful terminology and notation for the work that follows; we will not be studying the mathematical theory of sets as such. Relations arise in computing in the theory of relational databases, and we will need them in Chapter 12 when we study congruences.

The word *set* is used in mathematics to mean any well defined collection of items. The items in a set are called the *elements* of the set. For example, we can refer to the set of all the employees of a particular company, the set of all ASCII characters[1], or the set of all the integers that are divisible by 5.

A specific set can be defined in two ways. If there are only a few elements, they can be listed individually, by writing them between braces ('curly' brackets) and placing commas in between. For example, the set of positive odd numbers less than 10 can be written in the following way:

$$\{1, 3, 5, 7, 9\}$$

If there is a clear pattern to the elements, an ellipsis (three dots) can be used. For example, the set of odd numbers between 0 and 50 can be written:

$$\{1, 3, 5, 7, \ldots, 49\}$$

Some infinite sets can also be written in this way; for example, the set of all positive odd numbers can be written:

$$\{1, 3, 5, 7, \ldots\}$$

---

1 The ASCII character set is a standard set of 128 characters, including letters, digits, punctuation marks, mathematical symbols and non-printing (control) characters. Each character has a unique numeric code from 0 to 127. The 8-bit binary equivalent of the numeric code is used in many computers for the internal representation of character data. (ASCII stands for American Standard Code for Information Interchange.)

A set written in any of these ways is said to be written in *enumerated form*.

The second way of writing down a set is to use a property that defines the elements of the set. Braces are used with this notation also. For example, the set of odd numbers between 0 and 50 can be written:

$$\{x: x \text{ is odd and } 0 < x < 50\}$$

The colon is read 'such that', so the definition reads 'the set of all x such that x is odd and $0 < x < 50$'. Recalling our work from the previous chapter, notice that the expression following the colon is a predicate containing the variable x. A set written in the form $\{x:P(x)\}$, where $P(x)$ is a predicate, is said to be written in *predicate form*.

Capital letters are commonly used to denote sets. For example, we can write:

$$A = \{1, 2, 3, 4, 5\}$$

$$B = \{x: x \text{ is a multiple of } 3\}$$

The symbol $\in$ means 'is an element of'. For example, if A and B are the two sets defined above, we can write $2 \in A$ and $15 \in B$. The symbol $\notin$ means 'is not an element of'; for example, $6 \notin A$ and $11 \notin B$.

Many (but by no means all) of the sets we will be dealing with are sets of numbers. Some sets of numbers arise sufficiently often that special symbols are reserved for them. The most important of these for our subsequent work are listed below:

- **N** is the set of natural numbers (or positive integers): $\{1, 2, 3, 4, ...\}$.
- **J** is the set of integers: $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$.
- **Q** is the set of rational numbers: $\{x: x = m/n$ for some integers m and $n\}$.
- **R** is the set of real numbers.

The sets **J** and **R** may remind you of the data types 'integer' and 'real', which arise in programming. We will not go into the details of the concept of typing here. However, it is important to understand that a careful distinction needs to be made between the elements of **J** or **R** and the representations of integers or real numbers in a computer. Data types in a computer are constrained by the technical limitations of computing hardware; we saw in Chapter 3 that there is a limit to the size (and, in the case of real numbers, the precision) of the numbers that can be represented. There is no such restriction in mathematics; we are quite free to imagine infinite sets of numbers, and it is often convenient to do so.

There are two more sets for which we will introduce special symbols. The first of these is the *null* set (or empty set), which is denoted by the symbol $\varnothing$, and which has no elements. (Note that the symbol $\varnothing$ is not the same as the Greek letter ϕ (phi).) The null set can be written in enumerated form, like this:

$$\{\}$$

Don't make the mistake of writing $\{\emptyset\}$ for the null set. The set $\{\emptyset\}$ is *not* the null set; it is a set with one element, and that element is the null set.

The null set can be written in predicate form using any predicate that is always false, for example, $\{x: x \neq x\}$.

It may seem strange to define the null set, and you might wonder why it is necessary to do so. Perhaps you had similar misgivings when you first learnt about the number 0 ('If there's nothing there, how can you count it?'). It will become clear as we proceed that we need the null set in our work.

The other set for which we will introduce a symbol is the *universal* set, denoted by $\mathscr{E}$. The term 'universal set' does not refer to a specific set, but rather to a set that contains all the elements arising in the problem at hand. The universal set can therefore change from one problem to another. For example, in a problem dealing with various sets of numbers, we might choose $\mathscr{E}$ to be **R**, the set of all real numbers.

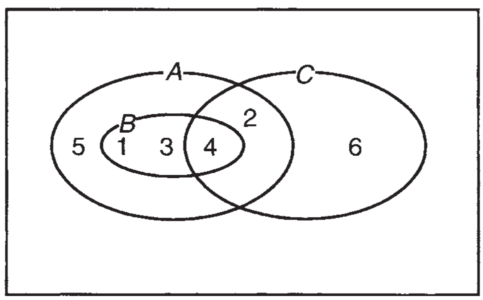
5.2 Subsets, set operations and Venn diagrams

Definition Let A and B be sets. We say that B is a *subset* of A, and write $B \subseteq A$, if every element of B is an element of A.

For example, let $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 3, 4\}$, and $C = \{2, 4, 6\}$. Then $B \subseteq A$, but C is not a subset of A, because $6 \in C$ but $6 \notin A$.

A useful way of depicting the relationship between several sets is to represent each set by an oval region on a type of diagram known as a *Venn*[2] *diagram*. The Venn diagram for the present example is shown in Figure 5.1.

Figure 5.1



The rectangle forming the boundary of the Venn diagram represents the universal set $\mathscr{E}$, which we may take to be $\{1, 2, 3, 4, 5, 6\}$ in this example.

2 Venn diagrams are named after the English mathematician, John Venn (1834–1923).

A second example of subsets is provided by the following 'chain' of subsets of **R**, the set of real numbers:

$$\mathbf{N} \subseteq \mathbf{J} \subseteq \mathbf{Q} \subseteq \mathbf{R}$$

The definition of 'subset' should be read carefully (as should all definitions in mathematics); it really does mean *exactly* what it says. In particular, if A is any set, then $A \subseteq A$, because it is certainly true that every element of A is an element of A. (The resemblance of the symbol $\subseteq$ to $\leq$ is not accidental; the relations 'subset' and 'less than or equal to' have some similar properties.)

The reasoning that underlies the following fact is a little more subtle:

$$\varnothing \subseteq A \text{ for any set } A$$

In words: *every element of* $\varnothing$ *is an element of* A. If you are puzzled by this statement, ask yourself how one set can *fail* to be a subset of another. This can happen only if there is an element of the first set that is not an element of the second; for example, {2, 4, 6} is not a subset of {1, 2, 3, 4, 5}, because 6 is an element of the first set but not the second. Therefore, the statement $\varnothing \subseteq A$ would be false *only* if we could find an element of $\varnothing$ that is not an element of A. But we can't find such an element, because $\varnothing$ has no elements! We say that the statement 'every element of $\varnothing$ is an element of A' is *vacuously* true, and conclude that $\varnothing \subseteq A$.

Now that we have established the concept of a subset of a set, we can define what it means for two sets to be equal.

Definition Two sets A and B are *equal* if $A \subseteq B$ and $B \subseteq A$.

In other words, $A = B$ if every element of A is an element of B, and every element of B is an element of A. A less formal way of expressing this is: 'Two sets are equal if they have the same elements.' In particular, this means that the order in which the elements of a set are listed in enumerated form is unimportant: {a, b, c} is the same set as {b, c, a}. It also means that a set does not have 'repeated' elements – we would never write a set as {a, a, b}, because it is the same set as {a, b}.

If $B \subseteq A$ and $B \neq A$, then B is called a *proper* subset of A.

A number of operations are defined on sets. We list them now, together with their corresponding Venn diagrams.

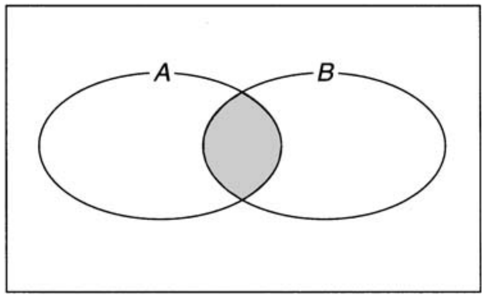
- The *intersection* of two sets A and B is:

$$A \cap B = \{x\colon x \in A \text{ and } x \in B\}$$

The intersection of A and B is depicted by the shaded region of the Venn diagram in Figure 5.2.

Two sets with no elements in common are said to be *disjoint*. In symbols, A and B are disjoint if $A \cap B = \varnothing$.

Figure 5.2



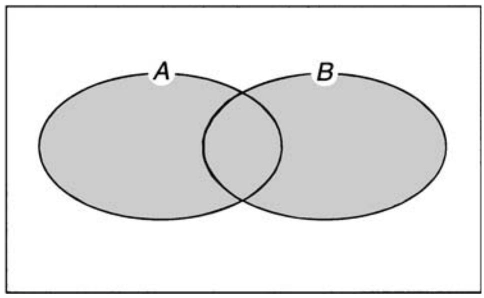
▶ The *union* of A and B is:

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

(Recall that 'or' always means inclusive-or.)

The union of A and B is depicted by the shaded region of the Venn diagram in Figure 5.3.

Figure 5.3



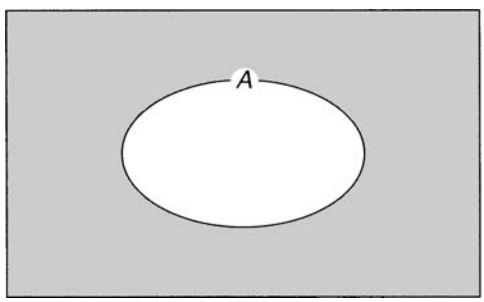
▶ The *complement* of A is:

$$\overline{A} = \{x : x \in \mathscr{E} \text{ and } x \notin A\}$$

(Recall that $\mathscr{E}$ is the universal set.)

The complement of A is depicted by the shaded region of the Venn diagram in Figure 5.4.

Figure 5.4

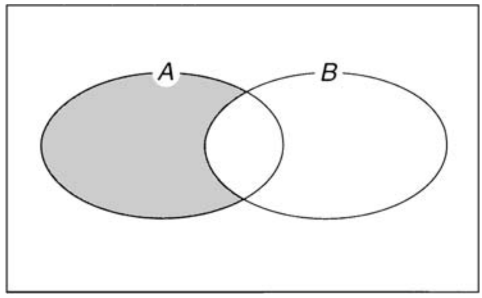


▶ The *difference* of A and B is:

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

The difference of A and B is depicted by the shaded region of the Venn diagram in Figure 5.5.

Figure 5.5

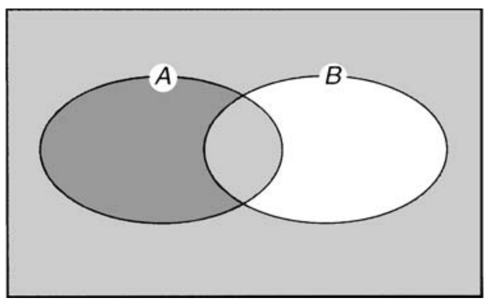


The last of these operations is less widely used than the others, because it can always be rewritten in terms of intersection and complement, using the law:

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

We can illustrate a law such as this one by constructing the Venn diagram for each side of the equation, and seeing that the two diagrams are the same. In this case, the Venn diagram for the right hand side is produced by shading the regions corresponding to A and $\overline{B}$, as shown in Figure 5.6. Then $A \cap \overline{B}$ corresponds to the doubly shaded region (indicated by darker shading in the figure). This region is the same as the region shaded in Figure 5.5.

Figure 5.6



Alternatively, we can prove that $A - B = A \cap \overline{B}$ using the definitions of the set operations:

$$A - B = \{x : x \in A \text{ and } x \notin B\} = \{x : x \in A\} \cap (x : x \notin B\} = A \cap \overline{B}$$

Example 5.2.1 Let the universal set be $\mathscr{E} = \{1, 2, 3, \ldots, 10\}$. Let $A = \{2, 4, 7, 9\}$, $B = \{1, 4, 6, 7, 10\}$, and $C = \{3, 5, 7, 9\}$. Find:

(a) $A \cup B$

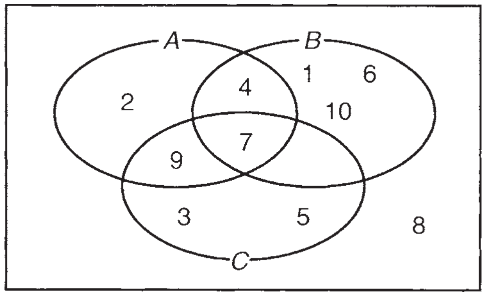
(b) $A \cap C$

(c) $B \cap \overline{C}$

(d) $(A \cap \overline{B}) \cup C$
(e) $\overline{B \cup C} \cap C$

Solution It is helpful to draw a Venn diagram in a problem like this (Figure 5.7).

Figure 5.7



(a) $A \cup B = \{1, 2, 4, 6, 7, 9, 10\}$
(b) $A \cap C = \{7, 9\}$
(c) $\overline{C} = \{1, 2, 4, 6, 8, 10\}$, so $B \cap \overline{C} = \{1, 4, 6, 10\}$
(d) $\overline{B} = \{2, 3, 5, 8, 9\}$, therefore $A \cap \overline{B} = \{2, 9\}$, so $(A \cap \overline{B}) \cup C = \{2, 3, 5, 7, 9\}$
(e) $B \cup C = \{1, 3, 4, 5, 6, 7, 9, 10\}$, therefore $\overline{B \cup C} = \{2, 8\}$, so $\overline{B \cup C} \cap C = \varnothing$

The operations of intersection, union and complement correspond in a natural way to the logical connectives **and**, **or** and **not** respectively. Because of this, each of the laws of logic gives rise to a corresponding law of sets.

For example, the commutative law $p \wedge q \equiv q \wedge p$ in logic yields the law $A \cap B = B \cap A$ for sets. We can show this in the following way:

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

The first and third equalities follow from the definition of the intersection of two sets, while the second equality follows from the commutative law of logic.

A list of some of the laws of sets is given in Table 5.1. Most of these laws have the same name as the corresponding law of logic, and all can be derived from one of the laws of logic in the way we have just seen.

Example 5.2.2 Use Venn diagrams to illustrate the first de Morgan's law for sets.

Solution We draw a Venn diagram for each side of the equation. For the left-hand side, we draw the Venn diagram for $A \cap B$ first, and then draw the Venn diagram for $\overline{A \cap B}$ (Figure 5.8).

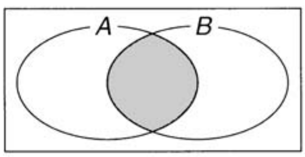
For the right-hand side, we draw the Venn diagrams shown in Figure 5.9.

The shaded region is the same for both sides of the equation.

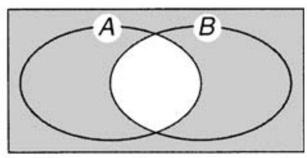
Table 5.1

Law(s)		*Name*
$\overline{\overline{A}} = A$		Double complement law
$A \cap A = A$	$A \cup A = A$	Idempotent laws
$A \cap B = B \cap A$	$A \cup B = B \cup A$	Commutative laws
$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$	Associative laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	de Morgan's laws
$A \cap \mathscr{E} = A$	$A \cup \varnothing = A$	Identity laws
$A \cap \varnothing = \varnothing$	$A \cup \mathscr{E} = \mathscr{E}$	Annihilation laws
$A \cap \overline{A} = \varnothing$	$A \cup \overline{A} = \mathscr{E}$	Inverse laws
$A \cap (A \cup B) = A$	$A \cup (A \cap B) = A$	Absorption laws

Figure 5.8

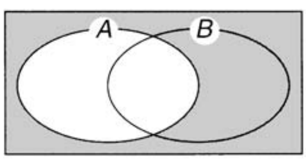


$A \cap B$

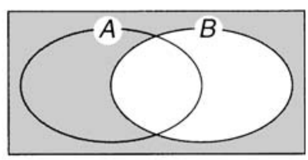


$\overline{A \cap B}$

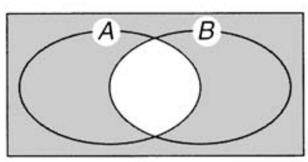
Figure 5.9



$\overline{A}$



$\overline{B}$



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

5.3 Cardinality and Cartesian products

Definition The *cardinality* of a finite[3] set is the number of elements in the set. The cardinality of a set A is denoted by $|A|$.

For example, if $A = \{a, b, c, d, e\}$ then $|A| = 5$.

Definition Let A be a set. The *power set* of A is the set of all subsets of A, and is denoted by $\mathscr{P}(A)$.

Note that a power set is an example of a *set of sets*; that is, a set whose elements are themselves sets.

For example, consider a set with three elements: {a, b, c}. Listing all the subsets of {a, b, c}, and remembering to include the set itself and the null set, we obtain the following power set:

$$\mathscr{P}(\{a, b, c\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

The power set of {a, b, c} has 8 elements. Since {a, b, c} can represent any 3-element set, we conclude that any set with 3 elements has 8 subsets.

The following result gives a general formula for the number of subsets of any finite set.

Theorem Let A be a set with n elements. Then A has 2^n subsets.

Proof Let $A = \{x_1, x_2, ..., x_n\}$, and suppose we want to select a subset B of A. We can do this by looking at each element of A in turn, and deciding whether or not to include it in B. There are two possibilities for x_1: either $x_1 \in B$ or $x_1 \notin B$. Similarly, either $x_2 \in B$ or $x_2 \notin B$ (2 possibilities), so the total number of possibilities for x_1 and x_2 is 2×2. Continuing in this way with $x_3, x_4, ..., x_n$, we conclude that the total number of possible subsets is $2 \times 2 \times ... \times 2$ (n times), which equals 2^n.

The technique used in the proof is an application of a result known as the Multiplication principle, which we will meet again in Chapter 9.

We noted earlier that the elements of a set are not listed in any particular order – {a, b} is the same set as {b, a}, for example. By contrast, an *ordered n-tuple* is a list of n elements *in a particular order*. To

3 It is possible to define cardinality for infinite sets also, but we will not do this here.

distinguish them from sets, ordered n-tuples are written using parentheses instead of braces:

$$(x_1, x_2, ..., x_n)$$

In particular, an ordered 2-tuple (usually called an *ordered pair*) is a pair of elements in a particular order, and is written (a, b). Thus, the ordered pair (1, 2) is different from (2, 1), for example.

If two ordered n-tuples $(x_1, x_2, ..., x_n)$ and $(y_1, y_2, ..., y_n)$ are equal, then the elements in the corresponding positions must be equal: $x_1 = y_1$, $x_2 = y_2$, and so on.

Definition The *Cartesian*[4] *product* of two sets A and B is defined by:

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$$

In words: $A \times B$ is the set of all ordered pairs in which the first element comes from A and the second element comes from B.

More generally, the Cartesian product of the n sets $A_1, A_2, ..., A_n$ is defined by:

$$A_1 \times A_2 \times ... \times A_n = \{(x_1, x_2, ..., x_n) : x_1 \in A_1, x_2 \in A_2, ..., x_n \in A_n\}$$

In words: $A_1 \times A_2 \times ... \times A_n$ is the set of all ordered n-tuples in which the first element comes from A_1, the second from A_2, and so on.

We can write the definition of $A_1 \times A_2 \times ... \times A_n$ more concisely by using predicate logic notation:

$$A_1 \times A_2 \times ... \times A_n = \{(x_1, x_2, ..., x_n) : \forall i \in \{1, 2, ..., n\}(x_i \in A_i)\}$$

The notation here is a little different from the notation in Chapter 4, because the set of values of i is written down explicitly here.

Example 5.3.1 Let $A = \{x, y\}$ and $B = \{1, 2, 3\}$. Write down the Cartesian product of A and B in enumerated form.

Solution

$$A \times B = \{(x,1), (x,2), (x,3), (y,1), (y,2), (y,3)\}$$

Cartesian products arise in computing when we deal with strings of characters defined according to certain rules. For example, on some computers, the usercode that identifies a registered user must consist of 3 letters, followed by 3 digits, followed by a letter, for example XYZ123A. Let L denote the set of letters, and let D denote the set of digits; then the set of all valid usercodes is:

4 The name comes from Cartesius, the latinised version of the name of the French mathematician and philosopher René Descartes (1596–1650).

$$L \times L \times L \times D \times D \times D \times L$$

The usercode XYZ123A corresponds to the element (X, Y, Z, 1, 2, 3, A) of the set $L \times L \times L \times D \times D \times D \times L$. (The difference between writing XYZ123A and (X, Y, Z, 1, 2, 3, A) is just one of notation, not a conceptual difference.)

Sometimes we want to form a Cartesian product of a set with itself. This situation arises sufficiently often to warrant a notation of its own. If A is any set, the Cartesian product $A \times A \times ... \times A$ (n times) is written A^n. Thus we can write:

$$A^n = \{(x_1, x_2, ..., x_n) : \forall i \in \{1, 2, ..., n\}(x_i \in A)\}$$

For example, $\mathbf{R}^2$ is the set of all ordered pairs of real numbers (x, y). In the study of coordinate geometry, this set is represented geometrically as a plane (the Cartesian plane), with x- and y-axes.

A second example, which we will use in Section 5.4, is the Cartesian product $\{0,1\}^n$. The elements of this set are ordered n-tuples in which each element is either 0 or 1. For example, (1, 0, 0, 1, 0, 1, 1, 1) is an element of $\{0,1\}^8$. We can think of $\{0,1\}^n$ as the set of all strings of n bits.

5.4 Computer representation of sets

Some programming languages, such as Pascal, allow sets to be handled as a compound data type, where the elements of the sets belong to one of the data types available in the language, such as integers or characters. The question then arises: how are sets stored and manipulated in a computer?

A set is always defined in a program with reference to a universal set $\mathscr{E}$. We must make an exception here to the rule that the order of the elements of a set is irrelevant, because we need to assume that the elements of $\mathscr{E}$ are listed in a definite order. Any set A arising in the program and defined with reference to this universal set $\mathscr{E}$ is a subset of $\mathscr{E}$. We want to know how the computer stores A internally.

The answer is that A is represented by a string of n bits, $b_1b_2...b_n$, where n is the cardinality of $\mathscr{E}$. In the notation we have just introduced, the bit string $b_1b_2...b_n$ can be regarded as the element $(b_1, b_2, ..., b_n)$ of $\{0,1\}^n$. The bits are determined according to the rule:

$b_i = 1$ if the ith element of $\mathscr{E}$ is in A

$b_i = 0$ if the ith element of $\mathscr{E}$ is not in A

where i ranges over the values 1, 2, ..., n.

Example 5.4.1 Let $\mathscr{E} = \{1, 2, 3, ..., 10\}$.

(a) Find the representation of {2, 3, 5, 7} as a bit string.

(b) Find the set represented by the bit string 1001011011.

Solution

(a) Looking in turn at each element of $\mathscr{E}$, and writing down 1 if the element is in {2, 3, 5, 7} and 0 if it is not, we obtain the answer: 0110101000.

(b) The answer is obtained by writing down each element of $\mathscr{E}$ that corresponds to a 1 in the bit string: {1, 4, 6, 7, 9, 10}.

Each subset of an n-element universal set $\mathscr{E}$ can be paired up with the n-bit string that is its computer representation. By doing this, we set up a one-to-one correspondence between the subsets of $\mathscr{E}$ and all possible n-bit strings. We know already that there are 2^n such strings, so there must also be 2^n subsets of $\mathscr{E}$. This provides another proof that any set with n elements has 2^n subsets.

The operations of intersection, union and complement can be carried out directly on the bit strings, provided that the sets involved have been defined with reference to the same universal set. For example, the bit string of $A \cap B$ has a 1 wherever the bit strings of A and B both have a 1. This process for calculating the bit string of $A \cap B$ is called a *bitwise* **and** operation. Similarly, the bit strings of $A \cup B$ and $\overline{A}$ are calculated using a bitwise **or** and a bitwise **not** respectively.

Example 5.4.2 Let the bit strings of A and B be 00101110 and 10100101 respectively. Find the bit strings of $A \cap B$, $A \cup B$ and $\overline{A}$.

Solution Performing the appropriate bitwise operations, we obtain the answers: 00100100, 10101111 and 11010001.

5.5 Relations

Relations between pairs of objects occur throughout mathematics and computing. We have already met some examples of relations. If one logical expression is equivalent to another, this is an example of a relationship between the two logical expressions. We can refer to the *relation* of one logical expression being equivalent to another. In a similar way, we can refer to the relation of one set being a subset of another. Other examples in mathematics are the relation of one number being less than another, and the relation of one integer being divisible by another. In a database in which words are to be sorted into alphabetical order, we deal with the relation of one word preceding another in an alphabetical listing. A non-mathematical example is the various relationships between members of a family – one person may be the sister of another, the cousin of another, and so on.

In each of these examples, a statement is made about a pair of objects that is true in some cases and false in others; the statement 'x is less than y' is true if $x = 3$ and $y = 4$, for example, but false if $x = 3$ and $y = 2$.

Before we can develop these ideas further, we need to make them more precise. We notice that each of the relations we have mentioned is associated with a set, and that the relation makes sense only when it refers to ordered pairs of elements of that set. For example, the relation 'less than' makes sense when it refers to ordered pairs of elements of **R**, the set of real numbers; if (x,y) is an ordered pair of real numbers, then the statement 'x is less than y' is either true or false. Similarly, the relation 'is a sister of' makes sense when applied to ordered pairs of elements of the set of all people, while the relation 'precedes in alphabetical order' refers to ordered pairs of words. In general, if the set to which the relation applies is denoted by A, then the ordered pairs are elements of the Cartesian product $A \times A$.

Informally, then, a relation on a set A is a statement about ordered pairs (x,y) belonging to $A \times A$. The statement must be either true or false for each pair of values of x and y. This is often the most convenient way of thinking about a relation. The formal mathematical definition is somewhat different, however.

Definition A *binary*[5] *relation* on a set A is a subset of $A \times A$.

This definition needs some explanation, since the connection between it and the informal idea of a relation might not be obvious. The easiest way to do this is by means of an example. Consider the relation 'less than' on the set $A = \{1, 2, 3, 4\}$. For any ordered pair of elements of A (that is, for any element of $A \times A$), the relation 'less than' is either true or false for that pair. We can list all of the ordered pairs for which the relation is true:

$$(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)$$

Formally, the relation is the set of these ordered pairs:

$$\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$$

This set is a subset of $A \times A$, and so it is a relation according to the definition given above.

If we denote this set of ordered pairs by R, then we can state that x and y are related by writing $(x, y) \in R$. In practice, it is more usual to write $x\ R\ y$ to mean that x and y are related. In fact, we don't even need the name R in this example – the relation already has its own symbol, '<', so we can simply write $x < y$ to mean that x is related to y.

There is a way of depicting a relation graphically that is often useful, provided that the set on which the relation is defined is not too large. This is done by using dots to represent the elements of the set, and drawing an

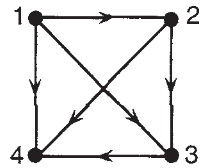
5 The word 'binary' refers to the fact that the relation is between *two* elements of A. As this is the only kind of relation we will be studying, we will omit the word 'binary' in what follows.

arrow from x to y for each pair (x,y) for which x is related to y. The resulting diagram is an object known as a *directed graph*.

Example 5.5.1 Draw the graphical representation of the relation 'less than' on {1, 2, 3, 4}.

Solution This is shown in Figure 5.10.

Figure 5.10



A relation on a finite set can also be represented as a rectangular array of Ts and Fs, known as a *relation matrix* (plural: *matrices*). The rows and columns of the matrix are labelled with the elements of the underlying set. If x is related to y, then the entry in the row labelled x and the column labelled y is T, otherwise it is F. This representation is particularly useful if a relation is to be stored and manipulated in a computer.

Example 5.5.2 Write down the relation matrix for the relation in Example 5.5.1.

Solution

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} F & T & T & T \\ F & F & T & T \\ F & F & F & T \\ F & F & F & F \end{bmatrix} \end{array}$$

We can define different types of relations according to their properties. The most important of these for our future work are listed below.

Definitions Let R be a relation on a set A.

- R is *reflexive* if $x \; R \; x$ for all $x \in A$.
- R is *irreflexive* if there are no elements x of A for which $x \; R \; x$.
- R is *symmetric* if $x \; R \; y$ implies $y \; R \; x$, for all $x, y \in A$.
- R is *antisymmetric* if $x \; R \; y$ and $y \; R \; x$ imply $x = y$, for all $x, y \in A$.
- R is *transitive* if $x \; R \; y$ and $y \; R \; z$ imply $x \; R \; z$, for all $x, y, z \in A$.

The above definitions could all be written somewhat more concisely using the notation of predicate logic, at the expense of producing what might appear to some people as an 'alphabet soup' of mathematical symbols. For example, the last definition (transitivity) could be written:

$$\forall x \forall y \forall z \{[(xRy) \wedge (yRz)] \rightarrow (xRz)\}$$

This more concise form (or something similar) would be used in programming in a relational database, in logic programming, and in formal system specifications.

As a general rule, we will use whatever combination of English words and mathematical symbols seems to make the meaning clearest. In this case, the definitions are probably easier to understand in the form in which they are given.

Example 5.5.3

The following relations are defined on the set of all people. Classify them according to the definitions given above.

(a) 'is a sister of'
(b) 'is the father of'
(c) 'has the same parents as'

Solution

(a) This relation is not reflexive; in fact it is irreflexive, because no person can be her (or his!) own sister. It is not symmetric (if *X* is the sister of *Y* then *Y* need not be the sister of *X* – *Y* could be the brother of *X*), nor is it antisymmetric (*X* can be the sister of *Y* and *Y* the sister of *X*, without *X* and *Y* being the same person). It is not transitive either, because if *X* is the sister of *Y* and *Y* is the sister of *Z* then *X* need not be the sister of *Z*. (This is a bit subtle; can you see why it is true?)
(b) This relation is not reflexive, it is irreflexive, it is not symmetric, it is antisymmetric (in a vacuous sense – think about the truth table for **if-then**), it is not transitive.
(c) This relation is reflexive (and not irreflexive), symmetric (and not antisymmetric) and transitive.

Example 5.5.4

Classify the following relations, which are defined on the set **J** of integers:

(a) 'is less than or equal to'
(b) 'is divisible by'
(c) 'has the same parity as' (that is, both integers are odd or both are even)

Solution

(a) $x \leq x$ is always true, so the relation is reflexive (and not irreflexive). If $x \leq y$ then it is never the case that $y \leq x$ except when $x = y$, so the relation is antisymmetric (and not symmetric). If $x \leq y$ and $y \leq z$ then $x \leq z$, so the relation is transitive.

(b) This relation is reflexive and transitive, but neither symmetric nor antisymmetric. (To see that it is not antisymmetric, note that –2 is divisible by 2 and 2 is divisible by –2, but $2 \neq -2$.)

(c) This relation is reflexive, symmetric and transitive.

Look again at the last of the three relations in Examples 5.5.3 and 5.5.4. Both relations express an idea of 'sameness' – 'has the *same* parents as', 'is the *same* parity as'. Notice that these two relations are reflexive, symmetric and transitive.

Definition A relation that is reflexive, symmetric and transitive is called an *equivalence relation*.

An equivalence relation is a relation that expresses the idea that two elements are the same in some sense. The relation 'is equivalent to' on the set of logical expressions is another example of an equivalence relation – two logical expressions are equivalent if they have the same truth table.

If an equivalence relation is defined on a set, then the elements that are related to each other can be grouped together into subsets. For example, if the relation is 'has the same parents as', defined on the set of all people, then all the people with one particular set of parents form one subset, the people with another set of parents form another subset, and so on. (Some of the subsets may contain only one person.) Each person belongs to exactly one subset. We say that the set of all people has been *partitioned* into disjoint subsets.

In the same way, the set of integers can be partitioned into subsets in which all the elements have the same parity. There will be two subsets: the set of even numbers and the set of odd numbers.

The process of forming a partition will not work if the relation is not an equivalence relation. For example, 'less than' is not an equivalence relation (because it is neither reflexive nor symmetric), and it makes no sense to define a 'set of numbers that are all less than each other'.

These ideas are summarised in the following definition and theorem.

Definition Let A be a set. A *partition* of A is a set of subsets of A such that every element of A is an element of exactly one of the subsets.

Theorem Let A be a set, and let R be an equivalence relation on A. For each element x of A, let $E(x)$ be the subset of A defined by $E(x) = \{y \in A\colon y\ R\ x\}$. Then the set of all the subsets $E(x)$ is a partition of A.

The subsets $E(x)$ are called the *equivalence classes* of the relation R.

Example 5.5.5 illustrates these ideas. This example might seem rather abstract now, but we will refer to it again when we study modular arithmetic in Chapter 12. Modular arithmetic has important applications to topics such as information coding and the computer generation of pseudo-random numbers for simulation modelling.

Example 5.5.5 Let R be the relation on the set **J** of integers defined by the rule: $x\ R\ y$ if $x - y$ is divisible by 4 (that is, $x - y = 4n$ for some integer n). Show that R is an equivalence relation, and describe the equivalence classes.

Solution If x is any integer, then $x - x = 0$, which is divisible by 4. Therefore R is reflexive.

Suppose $x - y$ is divisible by 4. This means that there is an integer n such that $x - y = 4n$. Then $y - x = -4n$, which is divisible by 4. Therefore R is symmetric.

Suppose $x - y$ and $y - z$ are both divisible by 4. This means that there are integers m and n such that $x - y = 4m$ and $y - z = 4n$. Then $x - z = x - y + y - z = 4m + 4n = 4(m + n)$, which is divisible by 4. Therefore R is transitive.

Since R is reflexive, symmetric and transitive, R is an equivalence relation.

We begin the task of describing the equivalence classes by choosing an element of **J** and describing the equivalence class containing that element. Suppose we choose 0. The equivalence class $E(0)$ is $\{y \in \mathbf{J}: y\ R\ 0\}$; in words, it is the set of all the integers y such that $y - 0$ is divisible by 4. This is simply the set of all multiples of 4 (positive, negative and zero):

$$E(0) = \{..., -12, -8, -4, 0, 4, 8, 12, ...\}$$

Now we choose another element of **J**, say 1. Then $E(1)$ will contain all the integers y such that $y - 1$ is divisible by 4:

$$E(1) = \{..., -11, -7, -3, 1, 5, 9, 13, ...\}$$

In the same way, we can find the equivalence class containing 2:

$$E(2) = \{..., -10, -6, -2, 2, 6, 10, 14, ...\}$$

Finally, we have the equivalence class containing 3:

$$E(3) = \{..., -9, -5, -1, 3, 7, 11, 15, ...\}$$

The process of finding the equivalence classes stops here, because the equivalence class containing 4 has already been found; it is the same as the one containing 0. Notice that the four equivalence classes form a partition of **J**, because every integer can be found in exactly one equivalence class.

It is worthwhile studying carefully the process we have used here to show that R is an equivalence relation, because this approach is used in similar problems. In order to show that a relation is an equivalence relation, we need to do three things:

- show that it is reflexive
- show that it is symmetric
- show that it is transitive

The first step is to determine what that means *for the particular relation given in the problem*. This means that the definitions of 'reflexive', 'symmetric' and 'transitive' must be interpreted for the problem at hand. For example, in order to show that a relation R is transitive, we must show that if $x\ R\ y$ and $y\ R\ z$ then $x\ R\ z$. In Example 5.5.5, this meant we had to show that if $x - y$ is divisible by 4 and $y - z$ is divisible by 4 then $x - z$ is divisible by 4. Once we have established what needs to be shown, we are already halfway there; the process of actually showing it is not necessarily difficult.

Before we leave equivalence relations, we will look at a (fairly informal) proof of the theorem that the equivalence classes $E(x)$ form a partition of A. In order to carry out the proof, we need to show that every element of A belongs to exactly one equivalence class.

It is easy to show that any element x of A belongs to *at least* one equivalence class. Since R is reflexive, we have $x\ R\ x$, so $x \in E(x)$.

Showing that no element belongs to more than one equivalence class takes a bit more work. We can do it using proof by contradiction. Suppose that $E(x)$ and $E(y)$ are two different equivalence classes, and suppose that they *do* have an element in common, say z. We now apply the following chain of reasoning:

Let w be any element of $E(x)$.

Then $w\ R\ x$ (by the definition of $E(x)$).

Since $z \in E(x)$, we also have $z\ R\ x$ (again using the definition of $E(x)$).

Therefore $x\ R\ z$ (because R is symmetric).

Since $w\ R\ x$ and $x\ R\ z$, we deduce that $w\ R\ z$ (because R is transitive).

Since $z \in E(y)$, we have $z\ R\ y$ (by the definition of $E(y)$).

Since $w\ R\ z$ and $z\ R\ y$, we deduce that $w\ R\ y$ (because R is transitive).

Therefore $w \in E(y)$ (by the definition of $E(y)$).

What we have just shown is that *any element of* $E(x)$ *must also be an element of* $E(y)$. A similar chain of reasoning shows that any element of $E(y)$ must be an element of $E(x)$ (just interchange the roles of x and y in the argument above). Therefore $E(x) = E(y)$, which contradicts the fact that $E(x)$ and $E(y)$ are two different equivalence classes. We conclude that the assumption that $E(x)$ and $E(y)$ have an element in common must be false. Therefore, no element of A can belong to more than one equivalence class.

Another type of relation, called a partial order relation, also occurs in many situations in computing. Its definition is given below.

Definition A relation is a *partial order* relation if it is reflexive, antisymmetric and transitive.

Here are some examples of partial order relations:

- The relation $\leq$ on the set of real numbers.
- The relation $\subseteq$ on the power set of a set.
- The relation 'is divisible by' on the set of natural numbers.
- The relation 'is a subexpression of' on the set of logical expressions (with a given set of variables).

As an example of the last one, p, q, $p \wedge q$, $\neg p$ and $(p \wedge q) \vee \neg p$ are the subexpressions of $(p \wedge q) \vee \neg p$.

If a partial order relation is defined on a set, we can regard the elements of the set as forming a hierarchy in which some elements are 'bigger' in some sense while others are 'smaller'. The word 'partial' refers to the fact that not all pairs of elements need to be related one way or the other; for example, if A and B are sets, it is not necessarily true that either $A \subseteq B$ or $B \subseteq A$. By contrast, it *is* true that if x and y are real numbers, then either $x \leq y$ or $y \leq x$; we express this fact by saying that $\leq$ is a *total* order relation on **R**.

Partial order relations occur in many areas of computing. One example arises if we have a computer program consisting of a number of modules: the main program, the subprograms called by the main program, the subprograms called by these subprograms, and so on. We can define a relation R on the set of modules $\{M_1, M_2, ..., M_n\}$, using the rule: $M_i \; R \; M_j$ if M_i is in the calling sequence of M_j (that is, M_j is the same module as M_i or M_j calls M_i or M_j calls a module that calls M_i or ...). You can check that R is reflexive and transitive. If R is not antisymmetric then circular calls are possible, such as two modules calling each other. The use of such 'recursive' calls must be avoided in programming languages that do not support recursion, but it can also be a powerful programming technique when it is available, as we will see when we study recursion in Chapter 7. If we are not using recursive calls, then R is a partial order relation.

EXERCISES

1 Write the following sets in enumerated form:

(a) The set of all vowels.

(b) $\{x \in \mathbf{N}: 10 \leq x \leq 20 \text{ and } x \text{ is divisible by } 3\}$

(c) The set of all natural numbers that leave a remainder of 1 after division by 5.

2 Write the following sets in predicate form:

(a) $\{4, 8, 12, 16, 20\}$

(b) {000, 001, 010, 011, 100, 101, 110, 111}

(c) {1, 4, 9, 16, 25, ...}

3 Let $A = \{1, \{1\}, \{2\}, 3\}$. Determine which of the following statements are true and which are false:

(a) $1 \in A$ (b) $1 \subseteq A$

(c) $\{1\} \in A$ (d) $\{1\} \subseteq A$

(e) $\{\{1\}\} \subseteq A$ (f) $2 \in A$

(g) $\{2\} \in A$ (h) $\{2\} \subseteq A$

(i) $\{3\} \in A$ (j) $\{3\} \subseteq A$

4 Let $\mathscr{E} = \{x \in \mathbf{N}: x \le 12\}$. Let $A = \{x: x \text{ is odd}\}$, $B = \{x: x > 7\}$, and $C = \{x: x \text{ is divisible by } 3\}$. Depict the sets on a Venn diagram. Hence write down the following sets in enumerated form:

(a) $A \cap B$

(b) $B \cup C$

(c) $\overline{A}$

(d) $(A \cup \overline{B}) \cap C$

(e) $\overline{A \cup C} \cup \overline{C}$

5 Illustrate the first distributive law, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, using Venn diagrams.

6 Illustrate the second absorption law, $A \cup (A \cap B) = A$, using Venn diagrams.

7 Show that $\overline{\overline{A} \cap B} = A \cup \overline{B}$ using the laws of sets.

8 Is the statement 'any set with n elements has 2^n subsets' true when $n = 0$?

9 Let $A = \{a, b, c\}$ and $B = \{p, q\}$. Write down the following sets in enumerated form:

(a) $A \times B$ (b) A^2 (c) B^3

10 Express each of the following sets as a Cartesian product of sets:

(a) The set of all possible 3-course meals (entrée, main course and dessert) at a restaurant.

(b) The set of car registration plates consisting of three letters followed by three digits.

(c) The set of all possible outcomes of an experiment in which a coin is tossed three times.

11 Let $\mathscr{E} = \{0, 1, 2, ..., 15\}$.

(a) Find the representation of {2, 4, 5, 7, 11, 14} as a bit string.

(b) Write down the set represented by the bit string 1010 0110 1110 1001.

(c) If A and B are represented by the bit strings 0011 0100 0110 1101 and 1010 1001 0001 0111, find the representations as bit strings of $A \cap B$, $A \cup B$, $\overline{A}$ and $\overline{B}$.

12 Write an algorithm to obtain the bit string representation of $A - B$ from the bit string representations of A and B, where A and B are subsets of a universal set $\mathscr{E}$ with n elements.

13 Consider the following algorithm:

1. Input a bit string b
2. $n \leftarrow$ the unsigned integer with b as its binary representation
3. $count \leftarrow 0$
4. **While** $n > 0$ **do**
   4.1. $n \leftarrow n \wedge (n-1)$
   {'∧' denotes bitwise 'and', applied here to the binary representations of n and $n-1$}
   4.2. $count \leftarrow count - 1$
5. Output *count*

Show that the output is the number of 1s in b. (You might find it helpful to trace the algorithm with a few different inputs first.)

14 Consider the following sequence of steps in pseudocode, where x and y are bit strings of equal length:

1. $x \leftarrow x \oplus y$ {⊕ denotes bitwise exclusive-or}
2. $y \leftarrow x \oplus y$
3. $x \leftarrow x \oplus y$

Show that the effect of the sequence of steps is to swap the values of x and y.

15 Let $A = \{1, 2, 3, 4, 5\}$, and let R be the relation on A defined as follows:

$$R = \{(1, 3), (1, 4), (2, 1), (2, 2), (2, 4), (3, 5), (5, 2), (5, 5)\}$$

(a) Write down the matrix representation of R.

(b) Draw the graphical representation of R.

16 Let R be the relation on {a, b, c, d} defined by the following matrix:

$$\begin{array}{c} \\ \text{a} \\ \text{b} \\ \text{c} \\ \text{d} \end{array} \begin{array}{c} \begin{array}{cccc} \text{a} & \text{b} & \text{c} & \text{d} \end{array} \\ \begin{bmatrix} \text{T} & \text{F} & \text{T} & \text{F} \\ \text{F} & \text{T} & \text{T} & \text{F} \\ \text{F} & \text{T} & \text{T} & \text{F} \\ \text{F} & \text{F} & \text{F} & \text{T} \end{bmatrix} \end{array}$$

(a) Draw the graphical representation of R.

(b) State, giving reasons, whether R is reflexive, symmetric or transitive.

17 Is the matrix representation of a relation unique, or could the same relation be represented by two different matrices?

18 Determine whether each of the following relations is reflexive, irreflexive, symmetric, antisymmetric or transitive:

(a) 'is a sibling (brother or sister) of', on the set of all people;

(b) 'is the son of', on the set of all people;

(c) 'is greater than', on the set of real numbers;

(d) the relation R on the set of real numbers, defined by $x\ R\ y$ if $x^2 = y^2$;

(e) 'has the same integer part as', on the set of real numbers;

(f) 'is a multiple of', on the set of positive integers.

19 Determine which of the relations in Exercise 18 are equivalence relations. For those that are equivalence relations, describe the equivalence classes.

20 Determine which of the relations in Exercise 18 are partial order relations.

21 A computer program consists of five modules: $M_1, M_2, \ldots, M_5$. A relation R on the set of modules is defined by the rule: $M_i\ R\ M_j$ if M_i is in the calling sequence of M_j. The relation matrix for R is shown below:

$$\begin{array}{c} \\ M_1 \\ M_2 \\ M_3 \\ M_4 \\ M_5 \end{array} \begin{array}{c} \begin{array}{ccccc} M_1 & M_2 & M_3 & M_4 & M_5 \end{array} \\ \begin{bmatrix} \mathrm{T} & \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{F} \\ \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{F} & \mathrm{F} \\ \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{F} & \mathrm{F} \\ \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{F} \\ \mathrm{F} & \mathrm{F} & \mathrm{T} & \mathrm{T} & \mathrm{T} \end{bmatrix} \end{array}$$

(a) Verify that R is reflexive, antisymmetric and transitive.

(b) Which module is the main program?