COMP235A: Logic and Computation

Sets, functions and relations.

1 Sets

Since the description of a *set* was stated by G. Cantor in 1895, the theory of sets has influenced many branches of mathematics. Here we shall not be looking at the mathematical theory of sets as such, but rather, we shall introduce some useful terminology and notation. As we shall see later, sets give rise to *relations* which have applications in such areas as relational databases.

Sets are used to group objects together. Much of the material that we cover on sets may be familiar to you already.

Definition 1 *A* set *is a well defined collection of distinct objects. The objects of a set are called the* elements *or* members *of the set. If a is a member of a set A, we say that a* belongs to *A and use the notation $a \in A$. On the other hand, if a does not belong to the set A, we write $a \notin A$.*

It is important that the objects be well defined. For example, "the collection of warm days in October" is not a set since the objects are not well defined.

A given set may be specified in several ways. If the set does not have too many members, it can be written down explicitly.

Example 1. The set containing the first five positive integers may be written as $A = \{1, 2, 3, 4, 5\}$.

If there is a clear pattern to the members, we may make use of an ellipsis (three dots) to specify a set.

Example 2. The set containing the 26 capital letters of the English alphabet may be written as $A = \{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Y}, \mathrm{Z}\}$.

A set written in any of these ways is said to be written in *enumerated form*. A second way of specifying a set is to give the property or properties that define a set.

Example 3. The set

$$A = \{x : 1000 < x \leq 2000\}$$

is the set of all numbers between 1000 and 2000, including 2000, but not 1000.

A set written in this way is say to be in *predicate form* or written in *set-builder notation*.

Many of the sets we have dealt with or will be dealing with are sets of numbers. These include the following:

- $\mathbb{N}$ is the set of natural numbers (that is, positive integers).
- $\mathbb{Z}$ is the set of all integers.

- $\mathbb{Q}$ is the set of all rational numbers (that is $\mathbb{Q} = \{x : x = a/b,\ a, b \in \mathbb{Z}, b \neq 0\}$).
- $\mathbb{R}$ is the set of real numbers.
- $\mathbb{C}$ is the set of complex numbers.

There is another set for which we introduce a special symbol. This is the *null* or *empty* set. As its name implies, it is the set which has no elements and we denote this set by $\emptyset$. It may be written in enumerated form as $\{\}$. Note that the set $\emptyset$ is not the same as the set $\{\emptyset\}$. The latter is a set with one element, namely $\emptyset$.

A set is *finite* if the number of elements in it is finite. Otherwise it is an *infinite* set. For a finite set, the *cardinality* of a set is the number of elements that belong to the set and we use $|A|$ to denote the cardinality of a set A. Thus $|\emptyset| = 0$.

Example 4. The set $A = \{\mathrm{A}, \mathrm{B}, \ldots, \mathrm{Y}, \mathrm{Z}\}$ given earlier is finite and has cardinality 26. The set $\mathbb{R}$ is an infinite set.

Definition 2 *A set A is a* subset *of a set B if every element of A is an element of B. We use the notation $A \subseteq B$.*

It is clear from this definition that $A \subseteq A$. If $A \subseteq B$ and there is at least one element of B that does not belong to A, then we say that A is a *proper subset* of B. It may be shown that $\emptyset \subseteq A$ for any set A.

Some books use the symbol $\subseteq$ to denote subset and $\subset$ to denote a proper subset. Here we shall use $\subseteq$ to denote both proper and improper subsets.

Example 5. We have $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Example 6. Let A be the set of vowels in the English alphabet and B be the set of letters in the English alphabet. It is clear that A is a proper subset of B.

One can also see from the definition of subset that the sets A and B are identical only if $A \subseteq B$ and $B \subseteq A$. In that case we write $A = B$.

2 Set operations

Two sets can be combined in many ways. For example, consider the set of students doing this algebra paper. Two subsets of this set are the set of students doing computer science papers and the set of students doing chemistry papers. We might want the set of students who are doing either chemistry or computer science papers or perhaps the set of students who are doing chemistry papers, but not computer science papers.

We now list the operations that may be defined on sets.

Definition 3 *The* intersection *of two sets A and B is*

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

In words, the intersection of A and B is the set of elements which belong to both A and B.

Example 7. Let A be the set of those students in this paper also doing computer science papers, and B be the set of those students in this paper also doing chemistry papers. Then $A \cap B$ is the set of students in this paper who are doing both computer science and chemistry papers.

Definition 4 *The sets A and B are said to be* disjoint *if $A \cap B = \emptyset$, that is, they have no elements in common.*

Example 8. Let A be the set of positive integers and B be the set of negative integers. Clearly A and B are disjoint sets.

Definition 5 *The* union *of A and B is*

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

In words, the union of A and B is the set of elements which belong to either A or B.

If A and B are both finite sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{1}$$

This formula is derived from the fact that if the cardinalities of A and B are added, then the elements in $A \cap B$ will be counted twice, so this is compensated for by subtracting $|A \cap B|$.

Example 9. With A and B are in Example 7, $A \cup B$ is the set of students in this paper who are doing either computer science papers or chemistry papers.

Definition 6 *The* complement *of $A \subseteq X$ is*

$$\bar{A} = \{x : x \in X \textit{ and } x \notin A\}.$$

In words, the complement of A is the set of elements in X which do not belong to A.

If both X and A are finite sets, then

$$|\bar{A}| = |X| - |A|. \tag{2}$$

Usually, X would be clear from the context.

Example 10. Let A be the set defined in Example 7 and X be the set of students in this paper. Then $\bar{A}$ is the set of students in this paper who are not doing any computer science papers.

Example 11. With the sets A and B as given in Example 7, suppose that there are 200 students in this paper, $|A| = 125$, $|B| = 67$, and $|A \cap B| = 50$. We want to find out how many of the 200 algebra students are not doing any computer science papers or chemistry papers. Thus we wish to find $|\overline{A \cup B}|$. From (1), we have

$$|A \cup B| = |A| + |B| - |A \cap B| = 125 + 67 - 50 = 142.$$

It then follows from (2) that the required answer is $200 - 142 = 58$.

Definition 7 *The* difference *of A and B is*

$$A \backslash B = \{x : x \in A \textit{ and } x \notin B\}.$$

In words, the difference of A and B is the set of elements which belong to A, but not to B.

It is not hard to show that if A, B are contained in some bigger set X,

$$A\backslash B = A \cap \bar{B}.$$

In any case, it is always true that if $B \subseteq A$, then

$$|A\backslash B| = |A| - |B|.$$

Theorem 8 *For any two sets A and B, $A\backslash B = A\backslash(A \cap B)$.*

To prove this we must show $A\backslash B \subseteq A\backslash(A \cap B)$ and also $A\backslash(A \cap B) \subseteq A\backslash B$.

For the first direction, suppose $x \in A\backslash B$. Then $x \in A$ and $x \notin B$, so certainly $x \notin A \cap B \subseteq B$. Hence $x \in A\backslash(A \cap B)$. Hence by definition, $A\backslash B \subseteq A\backslash(A \cap B)$.

Conversely, suppose $x \in A\backslash(A \cap B)$. Then $x \in A$ and $x \notin A \cap B$. We want to show $x \notin B$. Suppose rather that $x \in B$. Then $x \in A \cap B$ (since $x \in A$), a contradiction. So our assumption that $x \in B$ is wrong, so $x \notin B$. Since also $x \in A$, we have $x \in A\backslash B$, so by definition, $A\backslash(A \cap B) \subseteq A\backslash B$, completing the proof. □

Example 12. With the sets as given in Example 7, the set $A\backslash B$ is the set of students in this paper who are doing computer science papers, but not doing any chemistry papers. Using the values from Example 11, it is not hard to see that

$$|A\backslash B| = |A\backslash(A \cap B)| = |A| - |A \cap B| = 125 - 50 = 75 \text{ since } A \cap B \subseteq A.$$

3 Functions

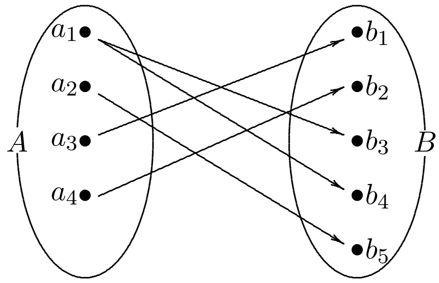
In many cases we assign to each element of a set a particular element of a second set (which may be the same as the first set). If you're doing calculus, then a familiar example is for a given real number, the assignment of another real number. Such an assignment is an example of a function. Though such functions may be graphed, there are other functions which are more general and not able to be graphed in the way that you are familiar with.

Definition 9 *Let A and B be sets. A* function *from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f : A \to B$.*

Example 13. Let $A = \{a_1, a_2, a_3, a_4\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$. Let g be the assignments from A to B given by

$$g(a_1) = b_3,\ g(a_1) = b_4,\ g(a_2) = b_5,\ g(a_3) = b_1,\ g(a_4) = b_2.$$

Though it is not obvious how to draw a graph of these assignments in the conventional sense, we can depict these assignments by use of an *arrow diagram*. This is given below and we see that g is *not* a function as a function cannot have more than one arrow emerging from any element of A.



Definition 10 *If f is a function from A to B, we say that A is the* domain *of f and B is the* codomain *of A. If $f(a) = b$, we say that b is the* image *of a. The* pre-image *of $b \in B$ is the set $\{a \in A \mid f(a) = b\}$, a subset of A which may be empty. The* range *of f is the set of all images of the elements of A. If f is a function from A to B, we say that f* maps A to B.

Just as for sets, there is a notion of equality for functions. Thus the functions $f_1 : A_1 \to B_1$ and $f_2 : A_2 \to B_2$ are *equal* if $A_1 = A_2$, $B_1 = B_2$, and $f_1(a) = f_2(a)$ for all $a \in A_1 = A_2$.

When f is a function from a set A to a set B, the image of a subset of A can also be defined:

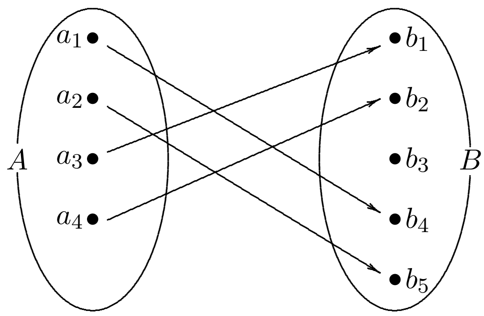
Definition 11 *Let f be a function from the set A to the set B. Suppose S is a subset of A. The* image *of S is the subset of B that consists of the images of the elements of S. We denote this by*

$$f(S) = \{f(s) : s \in S\}.$$

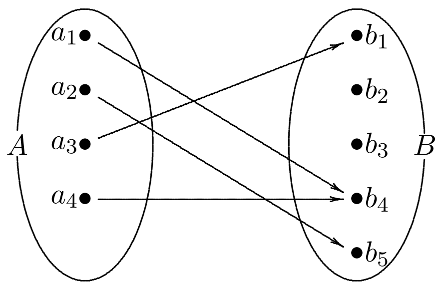
Some functions have distinct images at distinct members of the domain. Such a function is said to be one-to-one.

Definition 12 *A function f is said to be* one-to-one *or* injective *if and only if $f(a_1) = f(a_2)$ implies that $a_1 = a_2$ for all a_1, a_2 in the domain of f. A function is said to be an* injection *if it is one-to-one.*

Another way of expressing this idea is that f is one-to-one if and only $f(a_1) \neq f(a_2)$ whenever $a_1 \neq a_2$. It is sometimes important that a function be one-to-one. For example, consider a function which maps from the set of all possible original messages to the set of all encrypted secret messages. If the function is not one-to-one, then it is possible that two different messages could result in the same encrypted message. Obviously, there are going to be difficulties when it comes to decryption. A one-to-one function is shown in the arrow diagram below.

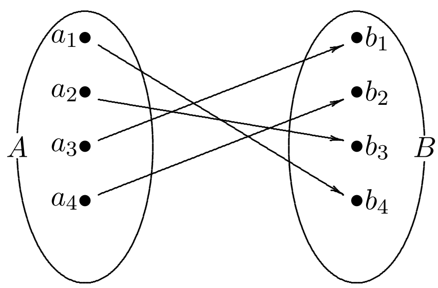


The function shown in the following arrow diagram is not one-to-one as there are two arrows which go to b_4.



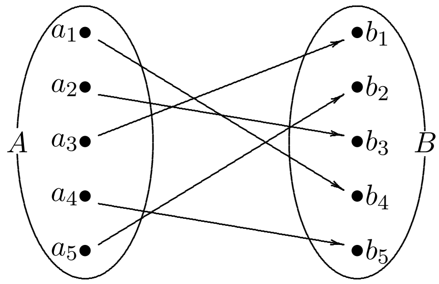
Definition 13 *A function f is said to be* onto *or* surjective *if and only if for every element $b \in B$, there is an element $a \in A$ for which $f(a) = b$. A function is said to be an* surjection *if it is onto.*

In other words, the function is onto if the range of f consists of the set B. Neither of the functions shown in the previous two arrow diagrams are onto. Here is an example of one that is.

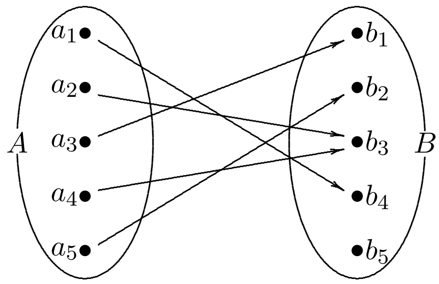


Definition 14 *If a function is both one-to-one and onto, then it is known as a* bijection.

The previous arrow diagram shows a bijective function as does the next one.



The next arrow diagram shows a function which is neither one-to-one nor onto.



Bijective functions have the important property that they have an inverse function. In more detail, since f is an onto function, then every element of B is the image of some element of A. Furthermore, because f is one-to-one, then every element of B is the image of a *unique* element of A. As a result, we can define a new function from B to A which reverses the mapping.

Definition 15 *Let f be a bijection from A to B. The* inverse function *of f is the function that assigns to each $b \in B$, the unique element $a \in A$ such that $f(a) = b$. We denote the inverse function by f^{-1}. Hence, $f^{-1}(b) = a$ when $f(a) = b$. In this situation, we say that f is* invertible.

Earlier on, we mentioned a function which maps from the set of all possible original messages to the set of all encrypted secret messages. We have already mentioned that it is important that such a function be one-to-one. It is also important that such a function be onto as well. If it were not, there would not be an inverse function meaning that there are encrypted messages that cannot be decrypted.

Another example is in compression and decompression of files. These processes are usually required on computers to save storage. A function which maps sets of files to sets of compressed files needs to be bijective. However, it is interesting to note that there is no file compression algorithm that compresses every file! A stronger statement is that any file compression algorithm that makes at least one file smaller must make at least one file larger!

Definition 16 *Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The* composition *of the functions f and g is denoted by $f \circ g$ and* *defined by*

$$(f \circ g)(a) := f(g(a)).$$

It is a mapping from the set A to the set C.

Composition satisfies some important properties. For example, it follows fairly easily that it is *associative*: if $h : A \to B$, $g : B \to C$ and $f : C \to D$ are all functions, then

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Definition 17 *Let A be a set. Denote by $I_A : A \to A$, the function which maps $a \in A$ to itself: $I_A(a) = a$ for all $a \in A$. This function is obviously bijective and is self-inverse.*

It is obvious that if $f : A \to B$ is a function, then

$$f = f \circ I_A = I_B \circ f.$$

Let $f : A \to B$ be a bijective function. Because of the way we have defined $f^{-1} : B \to A$, it should be clear that

$$f \circ f^{-1} = I_A \text{ and } f^{-1} \circ f = I_B.$$

In fact this last property can be used as a definition of when a function has an inverse, and it can then be shown that a function is invertible if and only if it is bijective.

4 Relations

Relationships between elements of a set occur in many contexts. For example, there is a relationship between each student in this class and his or her student ID number. Relationships between elements of a set may be represented using the structure called a *relation*. There are mathematical relations such as one number being less than another and non-mathematical relations such as relationships between members of a family—one person may be the sister of another, for example.

Before giving the definition of a relation, we need the concept of a Cartesian product.

Definition 18 *The* ordered pair (a_1, a_2) *is the ordered collection that has a_1 as its first element and a_2 as its second.*

Definition 19 *Let A and B be sets. The* Cartesian product *of A and B is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. We use the notation $A \times B$. Hence,*

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

Example 14. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$. Then

$$\begin{aligned} A \times B \quad = \quad & \{(1, \mathrm{a}), (1, \mathrm{b}), (1, \mathrm{c}), (2, \mathrm{a}), (2, \mathrm{b}), (2, \mathrm{c}), \\ & (3, \mathrm{a}), (3, \mathrm{b}), (3, \mathrm{c}), (4, \mathrm{a}), (4, \mathrm{b}), (4, \mathrm{c}), \\ & (5, \mathrm{a}), (5, \mathrm{b}), (5, \mathrm{c})\}. \end{aligned}$$

We can generalize the above definition to the Cartesian product of n sets $A_1, \ldots, A_n$. The Cartesian product is then

$$A_1 \times A_2 \times \cdots \times A_n = (a_1, a_2, \ldots, a_n),$$

where $a_i \in A_i$. The quantity $(a_1, a_2, \ldots, a_n)$ is known as an *ordered n-tuple*.

Definition 20 *Let A and B be sets. A* binary relation *from A to B is a subset of $A \times B$. We denote this set by $\mathcal{R}$. The notation $a\mathcal{R}b$ indicates that $(a, b) \in \mathcal{R}$, while the notation $a \not\mathcal{R} b$ indicates that $(a, b) \notin \mathcal{R}$. When $a\mathcal{R}b$, we say that b is related to a by $\mathcal{R}$.*

We define equality of relations in a straightforward way: they must be subsets of the same cartesian product $A \times B$, and must have the same ordered pairs in them.

In the previous section we considered functions. A function $f : A \to B$ may be thought of as a relation in $A \times B$ in which exactly one element of B is related to each element of A by $b = f(a)$, so f can be thought of as nothing but the relation $\{(a, f(a)) \mid a \in A\} \subseteq A \times B$.

For example, let $A = \{1, 2, 3, 4\}$ and $B = \{p, q, r\}$, and define

$$\mathcal{R}_1 = \{(1, q), (1, r), (2, p), (4, q)\}.$$

Note that this relation is not a function. (If it were, then $f(1)$ would have two values!)

Arrowgrams can be used to represent a relation $\mathcal{R} \subseteq A \times B$ also: simply draw an arrow from $a \in A$ to $b \in B$ if $(a, b) \in \mathcal{R}$.

Since a relation is a set, the usual set operations (such as union and intersection) may be applied to relations. But there are other operations as well, similar to those for functions.

Thus we can define the *converse* of a given relation $\mathcal{R} \subseteq A \times B$ to be the relation $\mathcal{R}^{-1} \subseteq B \times A$ by setting

$$\mathcal{R}^{-1} = \{(b, a) \mid (a, b) \in \mathcal{R}\}.$$

For our example,

$$\mathcal{R}_1^{-1} = \{(q, 1), (r, 1), (p, 2), (q, 4)\}.$$

The arrowgram simply has the arrows reversed.

Generally if $\mathcal{R}$ defines a function, $\mathcal{R}^{-1}$ is not a function, only a relation. But if $\mathcal{R}$ defines a bijective function, then $\mathcal{R}^{-1}$ is nothing but its inverse function.

We can compose relations in a way that generalises how we compose functions. If $\mathcal{R}_1 \subseteq A \times B$ and $\mathcal{R}_2 \subseteq B \times C$, then we define

$$\mathcal{R}_2 \circ \mathcal{R}_1 = \{(a, c) \mid a \in A, c \in C, \text{ and there exists } b \in B \text{ such that } (a, b) \in \mathcal{R}_1, (b, c) \in \mathcal{R}_2\}.$$

For example, letting A, B and $\mathcal{R}_1 \subseteq A \times B$ be as before, define also $C = \{*, +, \times\}$, and let $\mathcal{R}_2 = \{(q, *), (r, *), (p, +)\} \subseteq B \times C$. Then we can compute

$$\mathcal{R}_2 \circ \mathcal{R}_1 = \{(1, *), (2, +), (4, *)\}.$$

Note that $\mathcal{R}_1 \circ \mathcal{R}_2$ does not exist!

Of special interest to us are relations from a set A to itself. Such a relation is said to be a *relation on the set A*, and by definition, is a subset of $A \times A$. The above definition of a relation is quite formal and it is useful to informally think of a relation on a set A as a statement about ordered pairs (a_1, a_2) belonging to $A \times A$. The statement must be either true or false for each particular pair of values a_1 and a_2.

Example 15. Let $A = \{1, 2, 3\}$. We consider the ordered pairs in the relation

$$\mathcal{R} = \{(a_1, a_2) : a_1 \text{ is greater than } a_2\}.$$

Now we have

$$\begin{aligned} A \times A \quad = \quad & \{(1,1),(1,2),(1,3),(2,1),(2,2), \\ & (2,3),(3,1),(3,2),(3,3)\}. \end{aligned}$$

We then find that

$$\mathcal{R} = \{(2,1),(3,1),(3,2)\}.$$

Thus we can write $2\mathcal{R}1$, $3\mathcal{R}1$, and $3\mathcal{R}2$. In this example, we do not even need to use $\mathcal{R}$ as the relation already has its own symbol, namely '$>$'. Thus we can write $2 > 1$ to indicate that 2 and 1 are related by 2 being greater than 1.

For relations on a single set, there are other ways to represent them besides just arrow-grams: we can use *directed graphs* or *digraphs*, but we shall not consider these any further in this section.