

Chapter 1

Backgrounds

A *set* is a collection of objects. The objects collected in a set are called its *elements* or *members*. If a is a member of A , we write $a \in A$.

A set is called *finite* or *infinite*, if it contains either finite number or infinite number of elements. If a set is finite, it can be described by listing all of its members, e.g., $\{7, 21, 57\}$ is a finite set. Otherwise, we have to use a property to specify its members, e.g., $\{x \mid x \text{ is even}\}$.

Also, \mathcal{N} , the set of all the *natural numbers* is written $\{1, 2, 3, \dots\}$ and \mathcal{Z} , the set of all the *integers*, is written as $\{\dots, -2, -1, 0, 1, 2, \dots\}$.

Below are some of the often used operations and a relation regarding sets. Let A, B be two sets,

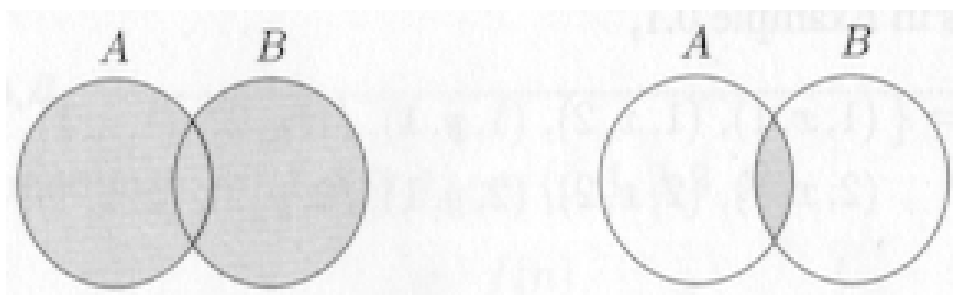
$$\text{Union } A \cup B = \{x | x \in A \vee x \in B.\}$$

$$\text{Intersection } A \cap B = \{x | x \in A \wedge x \in B.\}$$

$$\text{Complement } A - B = \{x | x \in A \wedge x \notin B.\}$$

$$\text{Subset } A \subseteq B \equiv \forall x, x \in A \Rightarrow x \in B.$$

As a visual aid, *Venn diagrams* are often used to specify these operations/relations among sets. For example, the following depicts the first two operations.



Homework: Exercise 0.1-0.3 in pp. 25–26.

Sequences and tuples

A *sequence* of objects is a list of these objects *in some order*. For example, $(7, 21, 57)$ represents the sequence 7, 21, 57.

Question: What is the difference between a set and a sequence?

Answer: Order.

A finite sequence with k elements is usually called a k -*tuple*. Particularly, a 2-tuple is called a *pair*.

For example, $(7, 21, 57)$ is a 3-tuple, while $(7, 21)$ is a pair.

Cartesian product

Let A, B be two sets, the *Cartesian product* of A and B is defined as follows:

$$A \times B = \{(a, b) | a \in A \wedge b \in B.\}$$

For example, if $A = \{1, 2\}$ and $B = \{x, y, z\}$, then

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

This operation is easily extended (?) to $k(\geq 3)$ sets.

Questions: What is $A \times B \times \{a, b, c\}$? What is the size of $A \times B \times C$, in general?

Homework: Exercise 0.4-0.5 in pp. 26.

Functions and relations

A *function* takes in one or more input(s) and sends out an output, e.g., $f(a) = b$. A function is a special *mapping* in the sense that the following always holds: for all x, y ,

$$x = y \Rightarrow f(x) = f(y).$$

Let f be a function, the collections of its possible inputs and outputs are called its *domain*, and *range*, respectively.

$$f : D \rightarrow R.$$

For example, the absolute value function, *abs*, is obviously a function in this sense. We have that:

$$\begin{aligned} \text{abs} : \mathcal{Z} &\rightarrow \mathcal{Z} \\ \text{abs}(x) &= \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{otherwise.} \end{cases} \end{aligned}$$

The above also provides a procedure (algorithm) to compute $\text{abs}(x)$ for any x .

Another way to describe a function is to use a table. For example,

$$f : \{0, 1, 2, 3, 4\} \rightarrow \{0, 1, 2, 3, 4\}.$$

and the following table describes f :

n	$f(n)$
0	1
1	2
2	3
3	4
4	0

When the domain of f is $A_1 \times \cdots \times A_k$, the input to f is a k -tuple (a_1, \dots, a_k) and is called an *argument* to f . When $k = 1, 2$, f is called a *unary* or a *binary* function, respectively.

Homework: Exercise 0.6 in pp. 26.

A *predicate* is a function whose range is $\{T, F\}$. For example, *even* is a predicate such that $even(x) = T$ iff x is an even number.

A *predicate* whose domain is a set of k -tuples is called a *relation*. In an expression involved with a binary relation, the latter is usually written as an infix notation. The statement aRb means that $aRb = T$. In general, $R(a_1, \dots, a_n)$ means that the latter is true.

Let R be a binary relation whose domain is D , it might have the following properties:

- R is *reflexive* iff for all $x \in D, xRx$.
- R is *symmetric* iff for all $x, y \in D, xRy \Leftrightarrow yRx$.
- R is *transitive* iff for all $x, y, z \in D, xRy$ and $yRz \Rightarrow xRz$.

Equivalent relations

A relation is *equivalent* iff it is reflexive, symmetric and transitive. For example, '=' is equivalent, but friendship is not.

As another example, let \equiv_7 be a relation with \mathcal{N} as its domain such that for all $i, j \in \mathcal{N}$, $i \equiv_7 j$ iff $i - j$ is a multiple of 7.

1) \equiv_7 is reflexive, because $0 (= i - i)$ is a multiple of 7.

2) \equiv_7 is symmetric, because if $i - j = 7q$ then $j - i = 7(-q)$.

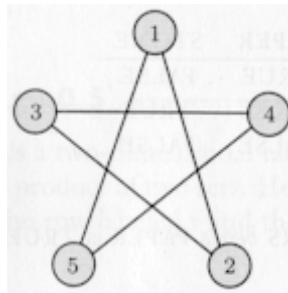
3) \equiv_7 is transitive, because if $i - j = 7q_1$ and $j - k = 7q_2$, then $i - k = (i - j) + (j - k) = 7(q_1 + q_2)$.

Thus, by definition, \equiv_7 is indeed equivalent.

Homework: Exercise 0.7 in pp. 26.

Graphs

As we discussed in detail in the data structure course, a *graph* is a set of points with lines connecting some of the points. The points are called *nodes* or *vertices*, while the connections are called *edges* or *links*. Below shows an example:

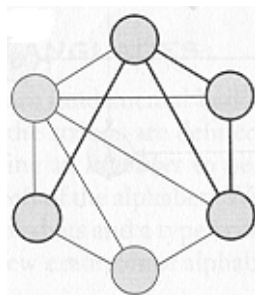


The above graph can be represented as

$$\begin{aligned} G &= (V, E) \\ &= (\{1, 2, 3, 4, 5\}, \{(1, 2), (1, 5), (2, 3), (3, 4), (4, 5)\}). \end{aligned}$$

Graphs can also be *labeled*, if we want to attach more information with the edges.

A graph G is a *subgraph of H* if the nodes of G is a subset of that of H and the edges of G are edges of H for the corresponding vertices. The following shows a (darker) subgraph.



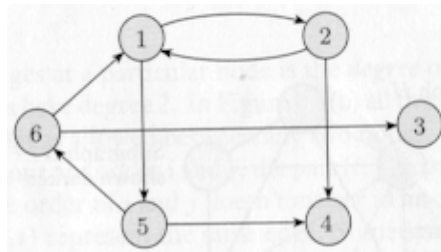
A *path* in a graph is a sequence of nodes connected by edges. A path is a *cycle* if it starts and ends at the same vertex. A *simple path* is a path in which no node repeats.

A graph is *connected* if every two vertices has a path between them.

A graph is a *tree* if it is connected and contains no cycles. We also have intuitive notions of *leaves* and *root*. A *forest* is a group of trees.

Homework: Exercise 0.8-0.9 in pp. 26–27.

We can also have *directed graph*, in which an edge is not a set, but an pair. Below shows a directed graph.



The street maps of many big cities such as Boston provide another example.

A path in which all the arrows point in the same direction is called a *directed path*. A directed graph is *strongly connected* if a directed path connects every two vertices.

Directed graphs are often used to describe binary relations. Let R be such a relation whose domain is $D \times D$, a labeled graph $G = (D, E)$ represents R , where $(x, y) \in E$ iff xRy .

Strings and languages

An *alphabet* is a finite set, generally denoted as Σ or Γ . For example,

$$\Sigma_1 = \{0, 1\}$$

$$\Gamma_1 = \{0, 1, x, y, z\}.$$

A *String* over an alphabet is a finite sequence of elements of that alphabet, e.g., 010001 is a string over Σ_1 . If w is a string over Σ , the *length* of w , written as $|w|$, is the number of symbols that it contains.

Particularly, the string of length 0, denoted as ϵ , is called the *empty string*.

If a string w has length n , it can be written as $w = w_1 \cdots w_n$. Then, its reverse is defined as $w^R = w_n \cdots w_1$.

A string, z , is a *substring* of w if z appears consecutively within w .

Let $x = x_1 \cdots x_m$ and $y = y_1 \cdots y_n$ be two strings, then the *concatenation* of x and y , written as xy , is the string $x_1 \cdots x_m y_1 \cdots y_n$.

A *language* over Σ is a set of strings over Σ .

The *lexicographic ordering* of strings is the same as the familiar dictionary ordering, except that shorter ones always precede the longer ones. For example, $abc \prec acb$, but $bc \prec abc$.

Definition, theorems and proofs

Definitions describe the objects and notions that we use. It could be simple or complicated, but it must be precise.

After definitions are given, we usually make some mathematical statements about the properties some objects might or might not have. A *proof* is a logic argument that a statement is true. It should be not only convincing, but correct beyond any doubt.

A *theorem* is a mathematical statement proven true. Sometimes, we prove a theorem only because it is needed in the proof of another statement. Such statements are called *lemmas*. Also, a theorem might lead us to conclude that other statements are true. The latter will be called the *corollaries* of the theorem.

An example

Definition: A graph is a *tree* if it is connected and contains no cycles.

Lemma: Any finite tree with at least two vertices has at least two leaves.

Proof: Since a tree is connected, there is a path between any two vertices. Take a longest path among all these paths. Let u be one of the two end points. Since it contains no cycles, u cannot be connected to any other vertex on the path. It is also true that u can't be connected to any vertex outside the path, since the path is a longest one. Thus, both of its two end points must be leaves.

Theorem: Any finite tree with $n(\geq 1)$ vertices must have $n - 1$ edges.

Proof by induction: Assume that $n = 1$, i.e., the tree contains only one node, obviously, it contains no edge.

Assume that tree, T , contains $n > 1$ nodes. By the lemma, T contains at least two leaves. Let one of them be l . Taking off l together with the edge connecting l to the rest of T , we have a sub graph of T , called T' . Since T contains $n - 1$ nodes, by the induction principle, T' has exactly $n - 2$ edges. Thus, T must have $n - 2$ edges.

Corollary: A forest with $n > 1$ nodes and $k > 1$ trees contains exactly $n - k$ edges.

Proof: Let $T_i, i \in [1, k]$, contain n_i nodes. By the Theorem, we have that e_i , the nodes of T_i , equals to $n_i - 1$. Hence,

$$e = (n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = n - k.$$

Looking for proofs

The only way to determine the truth of a mathematical statement is to prove it with a mathematical proof, which is usually difficult. Below are some general strategies.

1) Make sure that you understand the statement you want to prove.

For example, we often have to show that “ P iff Q ” where both P and Q are statements. It can be put into two parts. The first is “ P only if Q ”, which means “if P , then Q ”. The other is “ P , if Q ”. We clearly have to show both parts hold.

Another type is to show $A = B$, where both A and B are sets. Based on the definitions, we must prove that $A \subseteq B$ and $B \subseteq A$.

2) Try to get an intuitive feeling about why the statement should be true.

It is always a good idea to start with some small and/or simple examples. We will hit the jack pot if we find a *counterexample* which shows that the statement is actually false. We then have nothing else to do.

For example, given the statement that, *for all n , e_n is a prime number, where e_n is defined as follows:*

$$\begin{aligned}e_1 &= 2, \\e_n &= e_1 e_2 \cdots e_{n-1} + 1.\end{aligned}$$

Instead of giving a general argument, we test it out with $n = 1, 2, 3, \dots$ it turns out that the statement is false for $n = 5$, since

$$e_5 = 1807 = 13 \times 139.$$

If we are not lucky,...

,... you will have a much better understanding of the statement.

For example, given the statement that *for every graph G , the sum of the degrees of all the vertices is an even number.*

Begin with graphs with one, two or three edges, we gradually recognize that every edge increases this sum by 2.

3) When convinced a proof has been found, it must be written up properly so that other people can read it, verify it and accept it.

Examples

Theorem 0.10: For any two sets A and B ,
 $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof: We have to prove both $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$
and $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.

Assume that $x \in \overline{A \cup B}$. By definition, $x \notin A \cup B$.
Hence, $x \notin A$ and $x \notin B$, i.e., $x \in \overline{A}$ and $x \in \overline{B}$.
Thus, $x \in \overline{A} \cap \overline{B}$.

The other side is left as an exercise. □

Theorem 0.11: For every graph G , the sum
of the degrees of all the vertices is an even
number.

Proof: Every edge connects two nodes, thus,
contributes 2 to the sum of degrees of all the
nodes. Hence, if G contains e edges, the sum
is $2e$, an even number. □

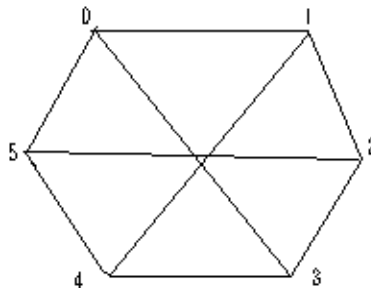
Types of proof

1. Proof by Construction. This technique is used to show the existence of objects that satisfy certain properties.

Theorem 0.12: For each even number of $n \geq 2$, there exists a 3-regular graph with n vertices.

Proof: Let n be such a number and construct $G = (V, E)$ with n nodes as follows: $V = \{0, 1, \dots, n-1\}$ and $E = \{(i, i+1) | i \in [0, n-2]\} \cup \{(n-1, 0)\} \cup \{(i, i + \frac{n}{2}) | i \in [0, \frac{n}{2} - 1]\}$. Q.E.D.

Below shows such a graph with $n = 6$.



2. Proof by Contradiction. To show that a statement is true, we assume that it is false first, and then show that this assumption leads to an obviously false consequence, a *contradiction*. Hence, the assumption must be false, i.e., the original statement must be true.

For example, let's prove that, for all $x > 0$,

$$x + \frac{4}{x} \geq 4.$$

Assume that for some $x > 0$, $x + \frac{4}{x} < 4$.

Since $x > 0$, we have that

$$\begin{aligned} x + \frac{4}{x} < 4 &\text{ iff } x^2 + 4 < 4x \\ &\text{ iff } x^2 - 4x + 4 < 0 \text{ iff } (x - 2)^2 < 0, \end{aligned}$$

which contradicts the fact that for all x ,

$$(x - 2)^2 \geq 0.$$

Hence, it must be the case that for all $x > 0$,

$$x + \frac{4}{x} \geq 4.$$

Another example

Theorem 0.14: $\sqrt{2}$ is irrational.

Proof: Just assume that for some integers m and n , we have that

$$\sqrt{2} = \frac{m}{n}.$$

W.l.o.g, m and n doesn't have any common divisor greater than 1. Particularly, they can't be both divided by 2.

Simple arithmetical manipulation leads to that $2n^2 = m^2$. Thus, m^2 must be even. Let it be $2k$. Thus, we have $2n^2 = 4k^2$, i.e., $n^2 = 2k^2$. Thus, n^2 is even as well. Therefore, both m and n must be even. A contradiction. \square

3. Proof by Induction. This technique can be used to show that all elements of an infinite set have a specified property. We usually apply it to \mathcal{N} , to show that every natural number has a property \mathcal{P} .

Every inductive proof to show that $\forall i \geq n_0, \mathcal{P}(i)$ consists of the following two steps: 1) $\mathcal{P}(n_0)$. and 2) $\forall i, \mathcal{P}(i) \Rightarrow \mathcal{P}(i + 1)$.

Step 1 is referred to as the *base case* and step 2 is the *inductive case*. Finally, the left-hand-side in step 2 is called the *inductive hypothesis*.

Below is the pattern in which an inductive proof is written:

Basis: Show that $\mathcal{P}(n_0)$ is true.

Inductive step: For each $i \geq n_0$, assume that $\mathcal{P}(i)$ is true and use this assumption to prove that $\mathcal{P}(i + 1)$ is true. . . .

Example

A simple result: for all $n \geq 1$,

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}.$$

Proof: Basis: Show that the equation is true when $n = 1$.

$$\sum_{i=1}^1 i = 1 = \frac{1 \times 2}{2}.$$

For each $n \geq 1$, assume that the equation holds, and prove it also holds for $n + 1$.

$$\begin{aligned} \sum_{i=1}^{n+1} i &= \sum_{i=1}^n i + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) = (n+1) \left[\frac{n}{2} + 1 \right] \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Thus, the equation holds for all $n \geq 1$. \square

Homework: Exercise 0.10, 11 and 12 in pp. 27.
Read through the proof of Theorem 0.15.