Discrete Mathematics 2007: Lectures 1 and 2
Sets Relations and Functions

Debrup Chakraborty

1 Sets: Basic Operations

The most frequently encountered object in mathematics is a *set*. A set is also encountered in our everyday life and is a commonly used word in our vocabulary. We speak of set of students in a class, set of sides of a polygon, the set of natural numbers etc. The concept of a set is so general that it is difficult to define it without replacing the word set for equivalent expressions like collection, aggregate etc.

The theory of sets itself is a rich and extensive subject area with its own peculiarities. But as said earlier sets forms a basic object in any mathematical discipline. So here we shall discuss some basic properties of set without going into the theoretical, philosophical and axiomatic aspects of the theory. For a gentle introduction to these aspects you are referred to the classic text by Halmos: *Naive Set Theory*.

We do not define sets here but assume that sets exists and represent collection of objects. The following notions and notations that follows will be central to our study of sets:

- We shall denote sets by uppercase alphabets like $A, B, \ldots$ and their elements by lowercase letters like $a, b, \ldots$.
- The symbol $a \in A$ will denote that the element a belongs to the set A and $a \notin A$ will denote that a do not belong to A. For example if we have the set $A = \{1, 2, 3, 4, 5\}$ then $5 \in A$ but $10 \notin A$.

- We say two sets A and B to be equal (denoted by $A = B$) if A and B has the same elements. For example $A = A$. Let

$$A = \{x : x \text{ is a root of the equation } x^2 - 5x + 6 = 0\}$$

and let $B = \{2, 3\}$, then $A = B$.

- If all the elements of a set A are also contained in another set B then we say that A is a *subset* of B and denote this by $A \subseteq B$. This definition includes the scenario when $A = B$. The notation $A \subset B$ denotes that A is a *proper subset* of B, which means that A is a subset of B but $A \neq B$, i.e., there exists at least one element in B which is not in A. For example if $\Re$ denotes the set of real numbers and $\mathbb{Z}$ denotes the set of integers then $\mathbb{Z} \subset \Re$.

  If $A \subseteq B$ and $B \subseteq A$ then $A = B$. We shall use this many times two prove equality of two sets.

- There exists a set with no element which is called the *null set* or the empty set or the void set. We shall denote a null set by the symbol ϕ. Every set contains ϕ as a subset.

1.1 Union and Intersection

If A and B are arbitrary sets, then their *union* is the set $C = A \cup B$ consisting of elements which belong to at least one of the sets A and B. Analogously we define the union of an arbitrary (finite or infinite) number of sets. If A_i are arbitrary sets, then $A = \cup_i A_i$ is the totality of the elements each of which belongs to at least one of the sets A_i.

The *intersection* of two sets A and B is the set $C = A \cap B$ which consists of all elements belonging to both A and B. For example, the intersection of the set containing all even integers with the set containing all integers which are multiples of 3, is the set of integers which are multiples of 6. The intersection of an arbitrary number of sets A_i is the set $A = \cap_i A_i$ which contains elements which belongs to all the sets A_i. For two sets A and B if $A \cap B = \phi$, we say A and B are disjoint, i.e. they have no element in common.

The operations of union and intersection are connected by the following relations:

Proposition 1. *Let A, B and C be sets. Then the following holds:*

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \tag{1}$$

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C) \tag{2}$$

Proof. We shall verify the first of the two relations and leave the other one as an exercise. Here we need to prove equality of two sets. So we shall begin with showing that

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$$

and then show that

$$(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C$$

and thus ultimately conclude the relation (1) of the proposition.

Let $x \in (A \cup B) \cap C$. This means that x belong to C and moreover belongs to at least one of the sets A and B. This is equivalent to saying that x belongs to at least one of the sets $A \cap C$ and $B \cap C$. Which further means that $x \in (A \cap C) \cup (B \cap C)$. So we have shown that $x \in (A \cup B) \cap C$ implies $x \in (A \cap C) \cup (B \cap C)$. In other words,

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C) \tag{3}$$

Similarly if $x \in (A \cap C) \cup (B \cap C)$. Then $x \in (A \cap C)$ or $xc \in (B \cap C)$. Consequently $x \in C$, and also x must belong to one of the sets A and B. So, $x \in (A \cup B) \cap C$. So we have showed that

$$(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C \tag{4}$$

So eq. (1) follows from equations (3) and (4). □

1.2 Set Difference

Now we shall talk of the operation for subtraction of sets. The difference of the sets A and B is the set $C = A \setminus B$ of those elements in A which are not contained in B. For example, if $A = \{x_1, x_2, x_3, x_4\}$ and $B = \{x_3, x_4, x_5, x_6\}$, then $A \setminus B = \{x_1, x_2\}$.

In some scenarios it is convenient to consider another kind of difference between sets, which is called the *symmetric difference*. The symmetric difference of two sets A and B

is defined as the union of the two sets $A \setminus B$ and $B \setminus A$. We shall denote the symmetric difference of A and B by the symbol $A \triangle B$, and its definition is symbolically written as

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

In various occasions we would need to consider various sets which are all subsets of some fundamental set U, which is usually called the *universal set*. In this case the set $U \setminus A$ is called the complement of A with respect to U. The next preposition which we state is of much importance in set theory and is called the principle of duality

Proposition 2. *1. The complement of an union is equal to the intersection of the complements,*

$$U \setminus \cup_i A_i = \cap_i (U \setminus A_i) \tag{5}$$

2. The complement of an intersection is equal to the union of the complements,

$$U \setminus \cap_i A_i = \cup_i (U \setminus A_i) \tag{6}$$

Proof. We give here a proof for Eq. 5, and leave the other as an exercise. Let $x \in U \setminus \cup_i A_i$, which means x that x does not belong to $\cup_i A_i$, i.e., it does not belong to any of the sets A_i. This suggests that x belongs to all of the sets $U \setminus A_i$. So $x \in \cap_i (U \setminus A_i)$. So we have proved that

$$U \setminus \cup_i A_i \subseteq \cap_i (U \setminus A_i).$$

Now, if $x \in \cap_i (U \setminus A_i)$ then x belongs to each of $(U \setminus A_i)$. So, it does not belong to any of A_i, i.e., it does not belong to $\cup_i A_i$. Which suggests that $x \in U \setminus \cup_i A_i$. So

$$\cap_i (U \setminus A_i) \subseteq U \setminus \cup_i A_i.$$

This completes the proof of Eq. 5. □

1.3 Cardinality

DEFINITION 1. For a finite set A, the cardinality of A is the number of elements in A and this is denoted by $|A|$.

If A and B be finite sets then

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

For three sets A, B, C, we shall have

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

We shall see this rule in more generality later

1.4 Cartesian Product

Given two sets A and B, the *cartesian product* of the sets is defined as

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

Thus, $A \times B$ is the set of ordered pairs (a, b) where $a \in A$ and $b \in B$. Also the pair (a_1, b_1) is said to be equal to (a_2, b_2), if and only if $a_1 = a_2$ and $b_1 = b_2$.

Given two sets A and B we can construct the products $A \times B$ and $B \times A$, and these sets are distinct. The cartesian product of a set A with itself is the set $A \times A$. If A is finite with n elements, then $A \times A$ contains n^2 elements.

2 Relations

A subset R of the set $A \times A$ is called a relation on A. A relation of specific interest to us is an *equivalence relation.*

A subset R of $A \times A$ is called an equivalence relation on A if

- $(a, a) \in R$ for all $a \in A$
- $(a, b) \in R$ implies $(b, a) \in R$
- $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$

Instead of talking of subsets of $A \times A$ we can conveniently talk of a binary relation on elements of the set A, i.e., when $(a, b) \in R$ we denote it by $a \sim b$ and call it as a related to b. With this notation we can restate the definition of a equivalence relation as below

DEFINITION 2. The binary relation $\sim$ on A is said to be a equivalence relation on A, if for all a, b and c in A,

- $a \sim a$ [Reflexivity]
- $a \sim b$ implies $b \sim a$ [Symmetry]
- $a \sim b$ and $b \sim c$ implies $a \sim c$ [Transitivity]

Example 1. Let S be a set and define $a \sim b$, for $a, b \in S$, if and only if $a = b$. This clearly defines a equivalence relation on S. In fact, an equivalence relation is generalization of equality, measuring equality up to some property.

Example 2. Let S be the set of all triangles in a plane. Two triangles are defined to be equivalent if they are similar (i.e., have corresponding angles equal). This defines a equivalence relation on S.

Example 3. Let S be the set of points in a plane. Two points a and b are defined to be equivalent if they are equidistant from the origin. This defines an equivalence relation on S.

Example 4. Let S be the set of all integers. Given $a, b \in S$, define $a \sim b$ if $a - b$ is an even integer. We verify that this is an equivalence relation of S.

1. Since $a - a = 0$ is even, so $a \sim a$
2. if $a \sim b$ then $(a - b)$ is even, then $b - a = -(a - b)$ is also even, so $b \sim a$
3. If $a \sim b$ and $b \sim c$ then $a - b$ and $b - c$ are even, whence $a - c = (a - b) + (b - c)$ is also even, thus $a \sim c$

DEFINITION 3. If A is a set and if $\sim$ is an equivalence relation on A, then the *equivalence class* of $a \in A$ is the set $\{x \in A : a \sim x\}$. We write it as $cl(a)$

Now let us see what are the equivalence classes in the examples that we just described. In Example 1, the equivalence class of a consists only of a. In Example 2 $cl(a)$ consists of all triangles which are similar to a. In Example 3, $cl(a)$ consists of all points in the plane which lie on a circle whose center is the origin and which passes through a. In Example 4, $cl(a)$ consists of all integers of the form $a + 2m$, where $m = 0, \pm 1, \pm 2, \ldots$.

Now we are ready to prove the first important theorem in this course.

Theorem 1. *Distinct equivalence classes of an equivalence relation on A provide us with a decomposition of A as an union of mutually disjoint subsets. Conversely, given a decomposition of A as an union of mutually disjoint, nonempty subsets, we can define an equivalence relation on A for which these subsets are the distinct equivalence classes.*

Proof. Let $\sim$ be a equivalence relation on A. For $a \in A$ let $cl(a)$ be the equivalence class of a. As $a \sim a$, thus, for all $a \in A$, $a \in cl(a)$. So, $\cup_{a \in A} cl(a) = A$. So we have proved that the union of the equivalence classes in A gives A.

Now, we need to show that for two distinct elements $a, b \in A$ either $cl(a) = cl(b)$ or $cl(a)$ and $cl(b)$ are disjoint. To show this let us assume that $cl(a)$ and $cl(b)$ have a non-empty intersection, and let $x \in cl(a) \cap cl(b)$. So, we have $x \in cl(a)$ and $x \in cl(b)$. Thus, by definition of a equivalence class we have $a \sim x$ and $b \sim x$. And $b \sim x$ implies $x \sim b$. Also, $a \sim x$ and $x \sim b$ together imply $a \sim b$. Now if $y \in cl(a)$ then $y \sim a$, also as $a \sim b$, so $y \sim b$, which means $y \in cl(b)$. Thus $y \in cl(b)$. So we conclude that $cl(a) \subseteq cl(b)$. This argument is symmetric and we can by the same argument conclude that $cl(b) \subseteq cl(a)$. Thus $cl(a) = cl(b)$. Thus we have proved that if $cl(a)$ and $cl(b)$ have a nonempty intersection then they must be equal.

To prove the other part of the theorem, we assume that A_α, $\alpha \in I$ be a decomposition of A such that $\cup_{\alpha \in I} A_\alpha = A$ and $A_\alpha \cap A_\beta = \phi$ for all $\alpha, \beta \in I$ s.t. $\alpha \neq \beta$. Now, we need to define an equivalence relation on A using this decomposition of A. For $a, b \in A$ we define $a \sim b$ iff a and b belongs to the same subset A_α. What is left is to prove that $\sim$ defined in the above manner is indeed an equivalence relation. We leave this as an exercise. $\square$

3 Functions

DEFINITION 4. If S and T are nonempty sets then a function from S to T is a subset, F, of $S \times T$ such that for every $s \in S$ there is an unique $t \in T$ such that the ordered pair $(s,t) \in F$.

The above definition precisely describes a function. But we would prefer to think a function as a rule which associates any element of S to some element in T. The rule being: *associate $s \in S$ with $t \in T$ if and only if $(s,t) \in F$*. We shall call t as the *image* of s under the function F.

We denote a function τ from S to T by the notation $\tau : S \to T$. If t is an image of s under τ then we shall usually write $\tau(s) = t$ [1].

Example 5. Let S be a set. Define $I : S \to S$ as $I(s) = s$ for all $s \in S$. I is called the identity function of S.

Example 6. Let $\mathbb{Q}$ be the set of rational numbers and let T be $\mathbb{Z} \times \mathbb{Z}$, where $\mathbb{Z}$ denotes the set of integers. Given $s \in \mathbb{Q}$, we can write $s = m/n$ where $m, n \in \mathbb{Z}$ such that they have no common factors. Define $\tau : \mathbb{Q} \to T$ as $\tau(s) = (m,n)$.

Example 7. Let S and T be sets; define $\tau : S \times T \to S$ by $\tau(a,b) = a$. This τ is called a projection of $S \times T$ on S. We can similarly define the projection of $S \times T$ on T.

Example 8. Define $\tau : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ as $\tau(a,b) = a + b$. This is an example of a *binary operation* on the set $\mathbb{Z}$. For a general set S, given a function $\tau : S \times S \to S$, we could use it to define a product $*$ in S by declaring $a * b = c$ if $\tau(a,b) = c$.

Example 9. Let $S = \{x_1, x_2, x_3\}$, define $\tau : S \to S$ by $\tau(x_1) = x_2$, $\tau(x_2) = x_3$ and $\tau(x_3) = x_1$

Example 10. Let $\mathbb{Z}$ be the set of integers and $B = \{0,1\}$. Define $\tau : \mathbb{Z} \to B$ as $\tau(x) = 1$ if x is even and $\tau(x) = 0$ if x is odd.

We shall have the opportunity to see many more examples as we proceed. But for the time being let us proceed with our discussion.

[1] Other notations are also in use like $t = \tau s$ or $s\tau = t$, the reader should be cautious about this while following other texts

DEFINITION 5. Given $\tau : S \to T$, the inverse image of $t \in T$ with respect to τ is the set $\{s : \tau(s) = t\}$.

For example in Example 10 the inverse image of 1 is the set of all even numbers. It can be so that for some element in T the inverse image with respect to a function τ is empty. As in Example 6 the inverse image of $(4, 2)$ is the empty set.

DEFINITION 6. The function $\tau : S \to T$ is called *onto* T if for any $t \in T$, there exists an $s \in S$ such that $\tau(s) = t$. An onto function is called a *surjection*.

DEFINITION 7. The function $\tau : S \to T$ is called *one-to-one* if whenever $s_1 \neq s_2$, then $\tau(s_1) \neq \tau(s_2)$. A *one-to-one* function is called an *injection*.

DEFINITION 8. A function which is both one-to-one and onto is called a *bijection*.

DEFINITION 9. The two functions σ and τ from S to T are called equal if for all $s \in S$, $\sigma(s) = \tau(s)$

Now let us suppose that there are two functions $\sigma : S \to T$ and $\tau : T \to U$. We now want to combine these two functions σ and τ to yield another function from S to U. The obvious way to do this is to first apply the function σ to obtain an element in T and then again apply τ to obtain an element in U. This operation is called *composition of functions* which is formally defined as follows:

DEFINITION 10. If $\sigma : S \to T$ and $\tau : T \to U$ then the composition of σ and τ is the function $\tau \circ \sigma : S \to U$ defined as $\tau \circ \sigma(s) = \tau(\sigma(s))$ for every $s \in S$.

Next we illustrate the composition operator with an example

Example 11. Let $S = \{x_1, x_2, x_3\}$ and let $T = S$. Let $\sigma : S \to S$ be defined by

$$\begin{aligned} \sigma(x_1) &= x_2 \\ \sigma(x_2) &= x_3 \\ \sigma(x_3) &= x_1 \end{aligned}$$

and $\tau : S \to S$ by

$$\begin{aligned}\tau(x_1) &= x_1\\ \tau(x_2) &= x_3\\ \tau(x_3) &= x_2\end{aligned}$$

Thus we have

$$\begin{aligned}\tau\circ\sigma(x_1) = \tau(x_2) &= x_3\\ \tau\circ\sigma(x_2) = \tau(x_3) &= x_2\\ \tau\circ\sigma(x_3) = \tau(x_1) &= x_1\end{aligned}$$

Lemma 1. *(Associative Law) If $\sigma : S \to T$, $\tau : T \to U$ and $\mu : U \to V$, then $\mu \circ (\tau \circ \sigma) = (\mu \circ \tau) \circ \sigma$*

Proof. First note that $\tau \circ \sigma$ makes sense and takes S to U, also $\mu \circ (\tau \circ \sigma)$ makes sense and takes S to V. Similarly $(\mu \circ \tau) \circ \sigma$ is meaningful and takes S to V. Thus we can talk of the equality or inequality of $\mu \circ (\tau \circ \sigma)$ and $(\mu \circ \tau) \circ \sigma$.

To show the equality, we must show that for any $s \in S$,

$$\mu \circ (\tau \circ \sigma)(s) = (\mu \circ \tau) \circ \sigma(s)$$

Now, from the definition of composition of functions we have

$$\begin{aligned}\mu \circ (\tau \circ \sigma)(s) &= \mu(\tau \circ \sigma(s))\\ &= \mu(\tau(\sigma(s)))\end{aligned}$$

Similarly,

$$\begin{aligned}(\mu \circ \tau) \circ \sigma(s) &= (\mu \circ \tau)(\sigma(s))\\ &= \mu(\tau(\sigma(s)))\end{aligned}$$

Thus we have $\mu \circ (\tau \circ \sigma)(s) = (\mu \circ \tau) \circ \sigma(s)$ for all $s \in S$. □

Now we shall prove two more important properties of functions:

Lemma 2. *Let $\sigma : S \to T$ and $\tau : T \to U$, then*

1. *$\tau \circ \sigma$ is a surjection if each of σ and τ are surjections.*

2. *$\sigma \circ \tau$ is an injection if each of σ and τ are injections*

Proof. 1. By hypothesis σ and τ are surjections, i.e., for every $t \in T$ there exists a $s \in S$ s.t. $\sigma(s) = t$ and for every $u \in U$ there exist a $t_1 \in T$ s.t. $\tau(t_1) = u$. So given any $u \in U$, we have a $s \in S$, s.t., $u = \tau(\sigma(s))$. So, $\tau \circ \sigma$ is a surjection.

2. Suppose $s_1, s_2 \in S$ and $s_1 \neq s_2$. As, σ is an injection, so $\sigma(s_1) \neq \sigma(s_2)$. And, τ being an injection $\tau(\sigma(s_1)) \neq \tau(\sigma(s_2))$. Which implies that for $s_1 \neq s_2$, $\sigma \circ \tau(s_1) \neq \sigma \circ \tau(s_2)$, which means that $\sigma \circ \tau$ is an injection.

□

Suppose $\sigma : S \to T$ is a bijection, i.e., it is both one-to-one and onto. For such a function we can define a function $\sigma^{-1} : T \to S$ by $\sigma^{-1}(t) = s$ if and only if $\sigma(s) = t$. We call σ^{-1} the inverse of σ. It is easy to verify that $\sigma^{-1} \circ \sigma$ is a function from S onto S, and similarly $\sigma \circ \sigma^{-1}$ is a function from T onto T. Now let $s \in S$, then $\sigma(s) = t$, for some t in T. Now, by definition $\sigma^{-1}(t) = s$, so

$$\sigma^{-1} \circ \sigma(s) = \sigma^{-1}(\sigma(s)) = \sigma^{-1}(t) = s.$$

We have shown that $\sigma^{-1} \circ \sigma$ is an identity function from S onto S. By a similar computation it can be shown that $\sigma \circ \sigma^{-1}$ is an identity function from T onto T.

Conversely, if $\sigma : S \to T$ is such that there exists a $\mu : T \to S$ with the property that $\mu \circ \sigma$ and $\sigma \circ \mu$ are identity mappings on S and T respectively then σ is a bijection. We formalize this in the next lemma:

Lemma 3. *The function $\sigma : S \to T$ is a bijection if and only if there exists a function $\mu : T \to S$ such that $\mu \circ \sigma$ and $\sigma \circ \mu$ are identity functions on S and T respectively.*

Proof. We have already shown that if σ is a bijection then there exist a function σ^{-1} such that $\sigma^{-1} \circ \sigma$ and $\sigma \circ \sigma^{-1}$ are identity functions on S and T respectively.

To prove the other way, we assume there exists a $\mu : T \to S$ with the property that $\mu \circ \sigma$ and $\sigma \circ \mu$ are identity mappings on S and T respectively. So for a given $t \in T$,

$\sigma \circ \mu(t) = \sigma(\mu(t)) = t$, so for any $t \in T$, t is the image of $\mu(t) \in S$ under the function σ. This shows that σ is onto. Further, if $\sigma(s_1) = \sigma(s_2)$ then we have

$$s_1 = \mu \circ \sigma(s_1) = \mu(\sigma(s_1)) = \mu(\sigma(s_2)) = \mu \circ \sigma(s_2) = s_2,$$

as $\mu \circ \sigma$ is a identity function on S. Thus we have shown that σ is one-to-one. Thus σ is a bijection.

□