Discrete Mathematics

Tapas Pandit

1 Propositional Calculus

In general, we are interested in validity of several (mathematical) statements. A statement may get complicated when it is composed of many statements. In propositional calculus, a complex statement is formed from many simple statements using *propositional connectives*: *negation* ($\neg$), *disjunction* (a.k.a "logical or") ($\vee$), *conjunction* (a.k.a "logical and") ($\wedge$), *conditional* ($\implies$) and *biconditional* ($\iff$).

A statement will have one of the two values, T (true) and F (false). For a complex statement, we have to consider *truth-functional* combinations of all the simple statements involved therein through different logical connectives. In the following, we illustrate validation of some statements.

Negation ($\neg$). If A is a statement, then its negation is denoted by $\neg A$. The truth-functional behavior of negation is given below using a table, called *truth table*.

A	$\neg A$
T	F
F	T

Disjunction ($\vee$). The disjunction of two statements A and B is denoted by $A \vee B$ and its truth table is given below.

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

Disjunction can easily be extended to more than two statements and the resultant statement will be true if and only if one of them is T.

Conjunction ($\wedge$). The conjunction of two statements A and B is denoted by $A \wedge B$ and its truth table is given below.

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

Conjunction can easily be extended to more than two statements and the resultant statement will be true if and only if all of them are T.

Conditional ($\implies$). The conditional connective of two statements A and B is denoted by $A \implies B$. We would read $A \implies B$ as "if A, then B". The statement $A \implies B$ is F when the *antecedent* A is T and the *consequent* B is F. The truth table of $A \implies B$ is given below.

A	B	$A \implies B$
T	T	T
T	F	F
F	T	T
F	F	T

What can be said about the validity of the following statements?

1. If $1 + 1 = 2$, then Plaksha University is located in Mohali, Punjab.
2. If $1 + 1 \neq 2$, then Plaksha University is located in Mohali, Punjab.
3. If $1 + 1 = 2$, then Plaksha University is located in New Delhi.
4. If $1 + 1 \neq 2$, then Plaksha University is located in New Delhi.

Biconditional ($\iff$). The biconditional connective of two statements A and B is denoted by $A \iff B$. We would read $A \iff B$ as "A if and only if B". The statement $A \iff B$ is T when A and B have the same truth value. The truth table of $A \iff B$ is given below.

A	B	$A \iff B$
T	T	T
T	F	F
F	T	F
F	F	T

Although we have already seen some statements constructed using some propositional connectives, there is a way to concretely define a statement form.

Definition 1.1. The propositional statement forms are defined recursively as follows.

1. All statement *letters* (capital) and such letters with numerical subscripts are statement forms.
2. If $\mathcal{X}$ and $\mathcal{Y}$ are statement forms, then so are $(\neg\mathcal{X})$, $(\mathcal{X} \vee \mathcal{Y})$, $(\mathcal{X} \wedge \mathcal{Y})$, $(\mathcal{X} \implies \mathcal{Y})$ and $(\mathcal{X} \iff \mathcal{Y})$.
3. Nothing is a statement form unless it follows from 1 and 2.

Here are some examples of statement forms: A, B_1, C_2, $(\neg B_2)$, $(D_{10} \wedge (\neg A))$, $(((\neg A) \vee B) \implies C)$, $((A \wedge B)) \implies (A \vee C))$ and $((A \iff B) \implies ((\neg A) \wedge B))$. Note that for every assignment of truth values T or F to the *statement letters* that appear in a statement form, there is a truth value for the statement form. Thus, each statement form determines a *truth function* (a.k.a *boolean function*). For example, look at the truth table of the statement form $(((\neg A) \vee B) \implies C)$.

A	B	C	$\neg A$	$((\neg A) \vee B)$	$(((\neg A) \vee B) \implies C)$
T	T	T	F	T	T
F	T	T	T	T	T
T	F	T	F	F	T
F	F	T	T	T	T
T	T	F	F	T	F
F	T	F	T	T	F
T	F	F	F	F	T
F	F	F	T	T	F

Remark 1.1. If there are n distinct letters involved in a statement form, then there are 2^n possible assignments of truth values to the statement letters and, hence, 2^n rows in the truth table.

If a statement always happens to be true, no matter what the truth values of its statement letters may be, then it is called a *tautology*. More concretely, it is defined as follows.

Definition 1.2 (Tautology)**.** A statement form is a *tautology* if its corresponding truth function takes only the value T, or equivalently, if in its truth table, the column under the statement form contains only T's.

Some examples of tautology are $(A \vee (\neg A))$, $(\neg(A \wedge (\neg A)))$, $(A \iff (\neg(\neg A)))$, $((A \wedge B) \implies A)$ and $(A \implies (A \vee B))$.

Definition 1.3 (Logically equivalent)**.** Two statement forms $\mathcal{X}$ and $\mathcal{Y}$ are said to be *logically equivalent* if they have the same truth table.

For example, A and $(\neg(\neg A))$ are logically equivalent.

Exercise 1.2. Check whether the following statements are tautologies.

1. $(((A \implies B) \implies B) \implies B)$
2. $(((A \implies B) \implies B) \implies A)$
3. $(((A \implies B) \implies A) \implies A)$
4. $(((B \implies C) \implies (A \implies B)) \implies (A \implies B))$
5. $((A \vee (\neg(B \wedge C))) \implies ((A \iff C) \vee B))$
6. $(A \implies (B \implies (B \implies A)))$
7. $((A \implies B) \vee (B \implies A))$
8. $((\neg(A \implies B)) \implies A)$

Exercise 1.3. Check whether the following pairs are logically equivalent.

1. $((A \implies B) \implies A)$ and A
2. $(A \iff B)$ and $((A \implies B) \wedge (B \implies A))$
3. $((\neg A) \vee B)$ and $((\neg B) \vee A)$
4. $(\neg(A \iff B))$ and $(A \iff (\neg B))$
5. $(A \vee (B \iff C))$ and $((A \vee B) \iff (A \vee C))$

2 Proofs by Contradiction

Proof by contradiction is proof strategy that proves the truth or the validity of a statement by showing that assuming the statement to be false leads to a contradiction.

Proposition 2.1. *Sum of odd integer and even integer is always an odd integer.*

Proof. Let o and e be odd and even integers respectively. We have to show that $o + e$ is an odd integer. Suppose otherwise, then $o + e$ is divisible by 2, which implies that $o + e = 2 \cdot m$ for some integer m. Then, $o = 2 \cdot m - e \implies o$ is an even integer, a contradiction. So, our assumption is wrong. Therefore, $o + e$ is an odd integer □

Proposition 2.2. *Sum of two odd integers is always an even integer.*

Proof. Let o_1 and o_2 be two odd integers. We have to show that $o_1 + o_2$ is an even integer. Suppose not, then $o_1 + o_2$ is an odd integer. We can write $o_1 + o_2 = 2 \cdot m + 1$ for some integer m. Also, we can write $o_2 = 2 \cdot n + 1$ for some integer n. So, we have $o_1 = 2(m - n)$ which implies that o_1 is an even integer, a contradiction. This completes the proof. □

Proposition 2.3. *The number of all primes is infinite.*

Proof. Suppose the number of all primes are finite. Let $p_1, p_2, \ldots, p_n$ be the list of all primes. Let $p = p_1 \cdots p_n$. Check that $p + 1$ is also a prime (why), which is not in the list. This is a contradiction. Therefore, the number of all primes are finite. □

Proposition 2.4. *Show that $\sqrt{2}$ is irrational.*

Proof. Suppose $\sqrt{2}$ is not irrational. Then, we can write $\sqrt{2} = p/q$ for some integers p and q with $\gcd(p, q) = 1$. So, we have $p^2 = 2 \cdot q^2 \implies p^2$ is even, which implies p is even integer. So, $4|p^2 \implies 4 \cdot q^2 \implies 2|q^2$ and hence, q^2 is even, implies q is even. So, $\gcd(p, q) \neq 1$, a contradiction. This completes the proof. □

Proposition 2.5. *Let o be an integer. Show that $o + 2$ is an odd integer if and only if o is an odd integer*

Proof. **If part.** Given that $o + 2$ is an odd integer. We have to show that o is odd. Suppose not, then $2|o \implies 2|(o + 2)$. So, $o + 2$ is an even integer which is a contradiction.

Converse. Given that o is an odd integer. We have to show that $o + 2$ is odd. Suppose not, then $o + 2$ is even. That means, $2|o$ which is a contradiction. □

Proposition 2.6. *Let A and B be two statements. Then $A \implies B$ if and only if $\neg B \implies \neg A$.*

Proof. **If part.** We show that if $A \implies B$, then $\neg B \implies \neg A$. Given $A \implies B$ and assume that $\neg B$ is true, that is, B is false. We have to show that $\neg A$ is true. Suppose otherwise, then A is true which implies that B is true (using $A \implies B$). This leads to a contradiction as B is false. So, $\neg A$ false and hence, $\neg B \implies \neg A$.

Converse. We have to show that if $\neg B \implies \neg A$, then $A \implies B$. In fact, by "if part", we have $\neg(\neg A) \implies \neg(\neg B)$. Since $\neg(\neg A)$ (resp. $\neg(\neg B)$) is equivalent to A (resp. B), the proof is done. □

3 Basics of Set Theory

A set is some collection of objects. Typically, sets are written within curly braces $\{, \}$. For example, $\{2, 4, 6, \ldots\}$ is the set of all positive even integers. Some conventional sets are given below.

- $\mathbb{R}$: Set of real numbers
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (Set of integers)
- $\mathbb{N} = \{1, 2, \ldots\}$ (Set of positive integers)

- $\mathbb{Q} = \{x \in \mathbb{R} : x = \frac{p}{q}, \text{ with } p, q \in \mathbb{Z} \text{ and } q \neq 0\}$ (Set of rational numbers)

Let us introduce some conventional notations of mathematics.

- for all: $\forall$
- there exists: $\exists$
- there exists unique: $\exists!$
- for $n \in \mathbb{N}$, define $[n] = \{1, 2, \ldots, n\}$

Membership. Given a set A and an element a, the notation "$a \in A$" means that "a belongs A" and the notation "$a \notin A$" indicates that "a does not belong to A".

Subset. We say a set A is a *subset* of B (denoted by $A \subseteq B$), if every element of A is also an element of B. That is, $A \subseteq B$, if $\forall x \in A \implies x \in B$. When A is not a subset of B, we write $A \nsubseteq B$. That is, $A \nsubseteq B$, if $\exists x \in A$ such that $x \notin B$.

Equality. For any two sets A and B, $A = B$ iff $A \subseteq B$ and $B \subseteq A$.

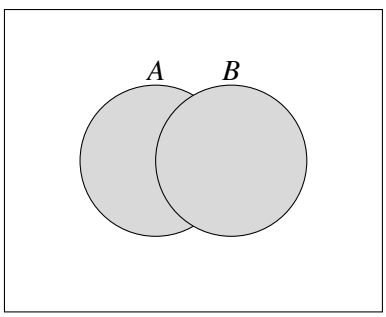
Empty set. A set without any element is called *empty set* and is denoted by $\emptyset$. So, $\emptyset = \{\}$. It is easy to check that $\emptyset \subseteq A$ for all sets A.

Cardinality. For a set A, its *cardinality*, denoted by $\#A$ or $|A|$, is defined to be the number of elements of A. A is called *finite set*, if $\#A \in \mathbb{N}$, otherwise, called *infinite set*.

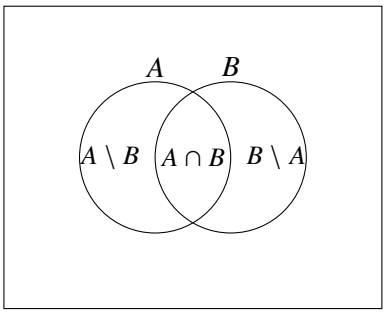
We now briefly discuss some basic set operations.

1. **Union.** For any two sets A and B, $A \cup B = \{x : x \in A \text{ or } x \in B\}$. This definition can be extended to any numbers of sets.
2. **Intersection.** For any two sets A and B, $A \cap B = \{x : x \in A \text{ and } x \in B\}$. This definition can be extended to any numbers of sets.
3. **Complement.** For a set A, its complement is defined by $\overline{A} = \{x : x \notin A\}$. That is, $x \in \overline{A} \iff x \notin A$.
4. **Set difference/minus.** For any two sets A and B, the set minus of A and B is defined by $A \setminus B = A \cap \overline{B} = \{x : x \in A \text{ and } x \notin B\}$.
5. **Symmetric difference.** For any two sets A and B, their symmetric difference is defined by $A \Delta B = (A \setminus B) \cup (B \setminus A)$. In other words, $A \Delta B = (A \cup B) \setminus (A \cap B)$.

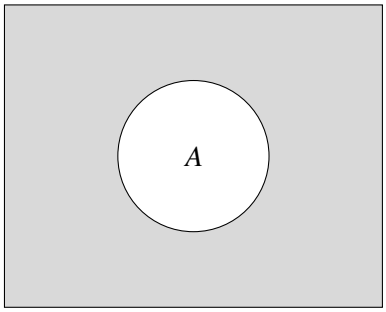
The Venn diagrams for union, intersection, complement and set and symmetric differences are given below.



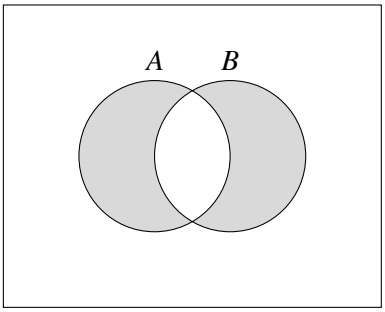
$A \cup B$



$A \setminus B, A \cap B$ and $B \setminus A$



$\overline{A}$



$A \Delta B$

Definition 3.1 (Set partition)**.** A partition of a given set A is a collections of nonempty sets $A_1, A_2, \ldots, A_k$ for some $k \in \mathbb{N}$ such that $A = \cup_{i=1}^{k} A_i$ and $A_i \cap A_j = \emptyset$ for any i, j with $1 \leq i, j \leq k$ and $i \neq j$.

It is easy to see that a set can be partitioned many ways. So, partition of a set is not unique. The above partition is called finite partition. This definition can be extended to infinite partition, if the the given set is infinite. For example, $\mathbb{N} = \cup_{i=1}^{\infty} A_i$, where $A_i = \{i\}$.

Next, we describe some universal laws which can be checked easily. Let A, B and C be any sets.

- **Associative.** $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$.
- **Commutative.** $A \cup B = B \cup A$ and $A \cap B = B \cap A$. Note that in general $A \setminus B \neq B \setminus A$.
- **Transitive.** If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
- **Subset.** $\emptyset \subseteq A \cap B \subseteq A$.
- **Complement.** $A \cap \overline{A} = \emptyset$ and $\overline{\overline{A}} = A$.
- **Idempotent.** $A \cup A = A \cap A = A$.
- **Dominance.** $A \cap \emptyset = \emptyset$ and $A \cup \emptyset = A$.
- **Absorption.** If $A \subseteq B$, then $A \cup B = B$ and $A \cap B = A$.
- **De Morgan's law.** $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$ and $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.
- **Distributive law.** $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- **Partition**. $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$. So, $A \setminus B$, $A \cap B$ and $B \setminus A$ form a partition for $A \cup B$.

Exercise 3.1. Let A, B and $\mathcal{S}$ be three sets such that $A, B \subseteq \mathcal{S}$. Prove that $A \cap B = \mathcal{S} \setminus ((\mathcal{S} \setminus A) \cup (\mathcal{S} \setminus B))$ and $A \cup B = \mathcal{S} \setminus ((\mathcal{S} \setminus A) \cap (\mathcal{S} \setminus B))$.

Power set. Let A be a set. Then, its *power set* is defined to be the set of all subsets of A (including the empty set $\emptyset$ and the set A itself). It is denoted by $\mathcal{P}(A)$ or 2^A, but the latter notation carries some meaningful information. Do you know what kind of information the 2nd notation carries? Let $A = \{a, b, c\}$, then its power set is $2^A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$. In this example, you might have noticed that $|2^A| = 8 = 2^{|A|}$. In fact, it can be shown that in general $|2^A| = 2^{|A|}$ using different approaches.

3.1 Cartesian Product

The Cartesian product of two nonempty[1] sets S and T is defined as $S \times T = \{(a, b) : \ a \in S \text{ and } b \in T\}$. Note that here (a, b) is an order pair and $(a, b) \in S \times T$ does not mean that $(b, a) \in S \times T$. Similarly, one can define Cartesian product $S_1 \times \cdots \times S_k$ of $S_1, S_2, \ldots, S_k$. Note that $|S_1 \times \cdots \times S_k| = |S_1| \cdot |S_2| \cdots |S_k|$.

Definition 3.2 (Binary Relation)**.** A binary relation between two sets S and T is subset $\mathcal{R}$ of $S \times T$. For any $(a, b) \in S \times T$, we say "a is $\mathcal{R}$-related to b" if $(a, b) \in \mathcal{R}$, otherwise "a is not $\mathcal{R}$-related to b".

Here, S is called *domain* and T is called *codomain*. When a is $\mathcal{R}$-related to b and $\mathcal{R}$ is understood from the context, we write $a\mathcal{R}b$ for simplicity. On other hand, if a and b are not related, we write $a \not\mathcal{R}\ b$.

Example 3.2. Let $S = \{1, 2, 3, 4, 5\}$ and $T = \{3, 4, 5, 6, 7, 8\}$. Let $\mathcal{R} = \{(a, b) \in S \times T : b - a = 5\}$, that is $\mathcal{R} = \{(1, 6), (2, 7), (3, 8)\}$.

[1] What happens if any of S and T is empty set?