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. □

Exercise 2.1. Prove the following using proof by contradiction.

1. Prove that $\sqrt{3}$ is irrational.
2. Prove that for any prime p, $\sqrt{p}$ is irrational.
3. Let m and n be two positive integers with $n > m$. Suppose n balls are thrown into m urns in such a way that each ball will get an urn. Prove that at least one urn contains more than one ball. Suppose there are n balls and m urns with $n > m$.
4. Let V be any vector space over $\mathbb{R}$. Show that any subset (resp. superset) of a linearly independent (resp. dependent) set in V is linearly independent (resp. dependent).

5. Consider the following system of linear equations over $\mathbb{R}$:

$$A\boldsymbol{x} = \boldsymbol{y}$$

where A is an $n \times n$ matrix, $\boldsymbol{x}$ is the column vector of unknown variables and $\boldsymbol{y} \in \mathbb{R}^n$ is a fixed column vector. Suppose the rank of A is less than n. Prove that the above system has more than one solution over $\mathbb{R}$.

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.

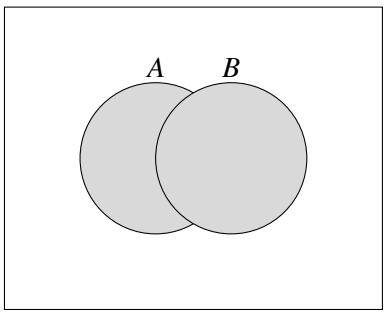
1. **Union.** For any two sets A and B, $A \cup B = \{x : x \in A \text{ or } x \in B\}$. This definition can be extended to any numbers of sets.
2. **Intersection.** For any two sets A and B, $A \cap B = \{x : x \in A \text{ and } x \in B\}$. This definition can be extended to any numbers of sets.

3. **Complement.** For a set A, its complement is defined by $\overline{A} = \{x : x \notin A\}$. That is, $x \in \overline{A} \iff x \notin A$.

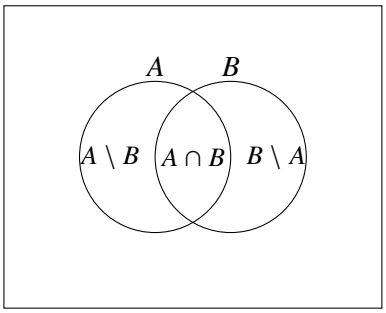
4. **Set difference/minus.** For any two sets A and B, the set minus of A and B is defined by $A \setminus B = A \cap \overline{B} = \{x : x \in A \text{ and } x \notin B\}$.

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, $A\Delta B = (A \cup B) \setminus (A \cap B)$.

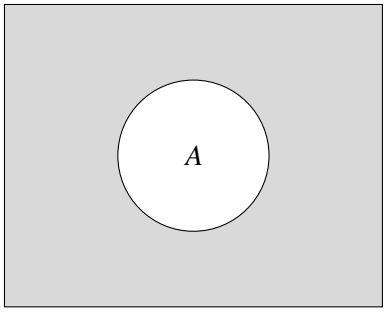
The Venn diagrams for union, intersection, complement and set and symmetric differences are given below.



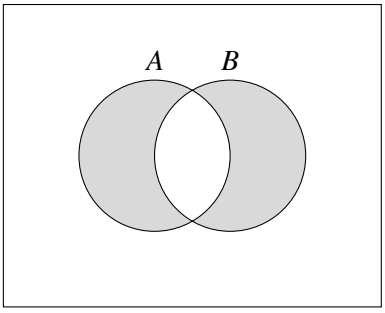
$A \cup B$



$A \setminus B, A \cap B$ 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 $\mathcal{R} = \{(1, 6), (2, 7), (3, 8)\}$.

4 Mathematical Induction

Mathematical induction (or simply induction) is an important tool for proving various mathematical statements $P(n)$ which depend on positive integer n. One of the widely use applications of it is proving formulas.

Theorem 4.1 (Mathematical induction)**.** *Let $P(n)$ be a statement about positive integers such that:*

1. *$P(1)$ is true.*
2. *If $P(k)$ happens to be true for some integers $k \geq 1$, then $P(k+1)$ is also true.*

Then, $P(n)$ is true for all $n \geq 1$.

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

Proof. Suppose that the theorem is false. Then, by well-ordering property[2], there exists a least integer $m \geq 1$ such that $P(m)$ is not true. Since $P(1)$ is true, so $m > 1$. Note that $1 \leq m-1 < m$. So, by choice of m, $P(m-1)$ is true. By the 2nd property (item 2), $P(m)$ is true, which is a contradiction. This completes the proof. □

The item 1 in Theorem 4.1 is called *initial/base/basis step*, whereas the item 2 is called *induction step*. The first part of the item 2, that is, "$P(k)$ happens to be true for some integers $k \geq 1$" is referred to as *induction hypothesis*. We now see some proofs of statements using mathematical induction.

1. Show that $1+2+\cdots+n = n(n+1)/2$. Let $P(n)$ denote the statement $1+2+\cdots+n = n(n+1)/2$. It is immediate that $P(1)$ is true. Let us assume that $P(k)$ for some $k \in \mathbb{N}$ (induction hypothesis). We show that $P(k+1)$ is true. In fact,

$$\begin{aligned} 1+2+\cdots+k+(k+1) &= (1+2+\cdots+k)+(k+1) \\ &= \frac{k(k+1)}{2}+(k+1) \text{ [by induction hypothesis: } P(k) \text{ is true]} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

2. Show that $3|(n^3-n)$ for all $n \geq 1$. Let $P(n)$ denote the statement $3|(n^3-n)$. It is immediate that $P(1)$ is true. Let us assume that $P(k)$ for some $k \in \mathbb{N}$ (induction hypothesis). We show that $P(k+1)$ is true. Indeed,

$$\begin{aligned} (k+1)^3-(k+1) &= k^3+3\cdot k^2+3\cdot k+1-(k+1) \\ &= k^3+3\cdot k^2+2\cdot k \\ &= k^3-k+3\cdot k^2+3\cdot k \\ &= (k^3-k)+3(k^2+k) \end{aligned} \tag{1}$$

   By induction hypothesis, the first term in the RHS of Equation 1 is divisible by 3 and obviously, the 2nd term is also divisible by 3. Therefore, $3|(k+1)^3-(k+1)$.

3. If p is prime and $p|a_1a_2\cdots a_n$, then show that $p|a_i$ for some $i \in [n]$. Let $P(n)$ denote the statement $p|a_1a_2\cdots a_n$. Obviously, $P(1)$ is true. Also, $P(2)$ is true. How? Let us assume that $P(k)$ is true for some k. We show that $P(k+1)$ is true, that is, if $p|a_1a_2\cdots a_ka_{k+1}$, then $p|p_i$ for some $i \in [k+1]$. We write $a_1a_2\cdots a_ka_{k+1} = a\cdot a_{k+1}$, where $a = a_1a_2\cdots a_k$. Now $p|a_1a_2\cdots a_ka_{k+1} \implies p|a\cdot a_{k+1}$. Since $P(2)$ is true, we have either $p|a$ or $p|a_{k+1}$. If $p|a$, then $p|a_i$ for some $i \in [k]$ (as $P(k)$ is true), otherwise, $p|a_{k+1}$. This completes this proof.

Exercise 4.1. Using induction solve the following problems.

1. Prove that $1^2+2^2+\cdots+n^2 = \frac{1}{6}\cdot n(n+1)(2n+1)$.
2. Let S and T be two sets with $|S| = |T| = n$. Then, show that the number injective functions from S to T is $n!$.
3. Show that the number of arrangements of n objects is $n!$.
4. Let A be s set with $|A| = n$. Then, show that $\mathcal{P}(A) = 2^n$.

[2]Every non-empty subset of $\mathbb{N}$ has least element.

5. Prove the binomial theorem, that is,

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i} \cdot b^i$$

for all $i \geq 1$.

6. Generalize Problem 2. That is, if p is any prime number, then show that $p|(n^p - n)$. Hint: binomial theorem.

5 Basics of Functions

Like sets, functions are also fundamental objects in mathematics. In the literature, functions are also know as maps or mappings.

Definition 5.1 (Function)**.** Let S and T be two nonempty sets. Then a function f from S to T, denoted by $f : S \to T$, is a binary relation on S and T such that for every $s \in S$, $\exists!\ t \in T$ such that the ordered pair (s,t) is in f. The unique point t is called the image of s under f, that is, $t = f(s)$. The sets S and T are called domain and codomain of f respectively.

Example 5.1. (**Identity.**) Let S be any set. Then, define $\mathbb{I}_S : S \to S$ by $f(s) = s$ for all $s \in S$. $\mathbb{I}_S$ is called identity function on S.

Example 5.2. (**Constant.**) Let S and T be two nonempty sets and $t_0 \in T$ be a fixed element of T. Let a function $f : S \to T$ be defined by $f(s) = t_0$ for all $s \in S$. This is called constant function.

Example 5.3. (**Projection.**) The function $f : S \times T \to S$ defined by $f(s,t) = s$ for all $(s,t) \in S \times T$ is called projection of $S \times T$ on S.

Example 5.4. Let $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ be defined by $f(s) = |s|$ (absolute value) $\forall s \in \mathbb{Z}$.

Example 5.5. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(s) = s + 1\ \forall s \in \mathbb{Z}$.

Example 5.6. Let $f : \mathbb{N} \to \mathbb{Z}$ be defined by

$$f(s) = \begin{cases} s/2 & \text{if } s \text{ is even} \\ (1-s)/2 & \text{if } s \text{ is odd.} \end{cases}$$

5.1 Injective, Surjective, Bijective, Composition, and Inverse

Let $f : S \to T$ be a function with domain S and codomain T. The range of f is defined by $f(S) = \{f(s) : s \in S\}$. Note that $f(S)$ is a subset of T. For an element $t \in T$, its inverse image is a set defined by $f^{-1}(t) = \{s \in S : f(s) = t\}$. Similarly, for an subset $A \subseteq T$, its inverse image set can be defined. In fact, $f^{-1}(A) = \{s \in S : f(s) \in A\}$.

Definition 5.2 (Injective)**.** A function $f : S \to T$ said to be injective (a.k.a one-one), if for any distinct $s_1, s_2 \in S$ we have $f(s_1) \neq f(s_2)$.

Exercise 5.7. Prove that a function $f : S \to T$ is injective if and only if $\forall t \in T$, $|f^{-1}(t)| \leq 1$.

Definition 5.3 (Surjective)**.** A function $f : S \to T$ said to be surjective (a.k.a onto) if $f(S) = T$.

Exercise 5.8. Prove that a function $f : S \to T$ is surjective if and only if $\forall t \in T$, $|f^{-1}(t)| \geq 1$.

Definition 5.4 (Bijective)**.** A function $f : S \to T$ said to be bijective (a.k.a 1-1 correspondence) if it is both injective and surjective[3].

Exercise 5.9. Prove that a function $f : S \to T$ is bijective if and only if $\forall t \in T$, $|f^{-1}(t)| = 1$.

Exercise 5.10. Prove or disprove that the functions defined in Examples 5.1 to 5.6 are bijective.

Definition 5.5 (Equality)**.** Two functions $f_1 : S \to T$ and $f_2 : S \to T$ are said to be equal, if $f_1(s) = f_2(s)$ for all $s \in S$.

Definition 5.6 (Composition)**.** Let $f : S \to T$ and $g : T \to U$ be two functions. Then, the composition of g and f is a function $g \circ f : S \to U$ defined by $(g \circ f)(s) = g(f(s))$ for all $s \in S$.

Note that in the above definition, we consider $\mathsf{Dom}(g) = \mathsf{Codom}(f) = T$. If we consider $f : S \to T_1$ and $g : T_2 \to U$ with $T_1 \neq T_2$, then the basic requirement for defining $g \circ f : S \to T$ is that $f(S) \subseteq \mathsf{Dom}(g) = T_2$.

Caveat. In general, $f \circ g \neq g \circ f$. Moreover, $f \circ g$ may not be definable. For example, let $f : S \to T$ and $g : T \to U$ be defined by $f(s) = 2s$ for $s \in S$ and $g(t) = t + 1$ for $t \in T$, where $S = \{1, 2, 3\}$, $T = \{2, 4, 6\}$ and $U = \{3, 5, 7\}$. It easy to check that $g \circ f : S \to U$ follows the rule: $(g \circ f)(s) = g(f(s)) = g(2s) = 2s + 1$ for $s \in S$. On the other hand, $f \circ g$ cannot be defined. Why?

Lemma 5.1. *Let $f : S \to T$ and $g : T \to U$ be two functions. Then, prove the following statements.*

1. *If f and g are surjective, then $g \circ f : S \to U$ is surjective.*
2. *If f and g are injective, then $g \circ f : S \to U$ is injective.*
3. *If $g \circ f : S \to U$ is injective, then f is injective.*
4. *If $g \circ f : S \to U$ is surjective, then g is surjective.*

Proof. Exercise. □

Corollary 5.2. *Let $f : S \to T$ and $g : T \to U$ be two functions. Then, the following statements hold.*

1. *If f and g are bijective, then so is $g \circ f : S \to U$.*
2. *If $g \circ f : S \to U$ is bijective, then f is injective and g is surjective.*

Proof. Immediate! □

Exercise 5.11. Let $f : S \to T$ and $g : T \to U$ be two functions. Then, disprove the following statements.

1. If $g \circ f : S \to U$ is surjective, then f is surjective.
2. If $g \circ f : S \to U$ is injective, then g are injective.
3. If f is injective and g is surjective, then $g \circ f : S \to U$ is bijective.

Typically, in mathematics we talk about inverse of an object. For example, inverse of 2 is 1/2 (w.r.t multiplication), because $(1/2) \cdot 2 = 1 = 2 \cdot (1/2)$. Notice that a function $f : S \to T$ associates each element of its domain S to an unique element from its codomain T. The very first question is what is the sense of inverse of a function? Note that composition of functions can be thought of multiplication. Can we formally define the inverse of $f : S \to T$ w.r.t composition of functions?

[3]Some examples of injective, surjective and bijective functions are given in Figure 1.

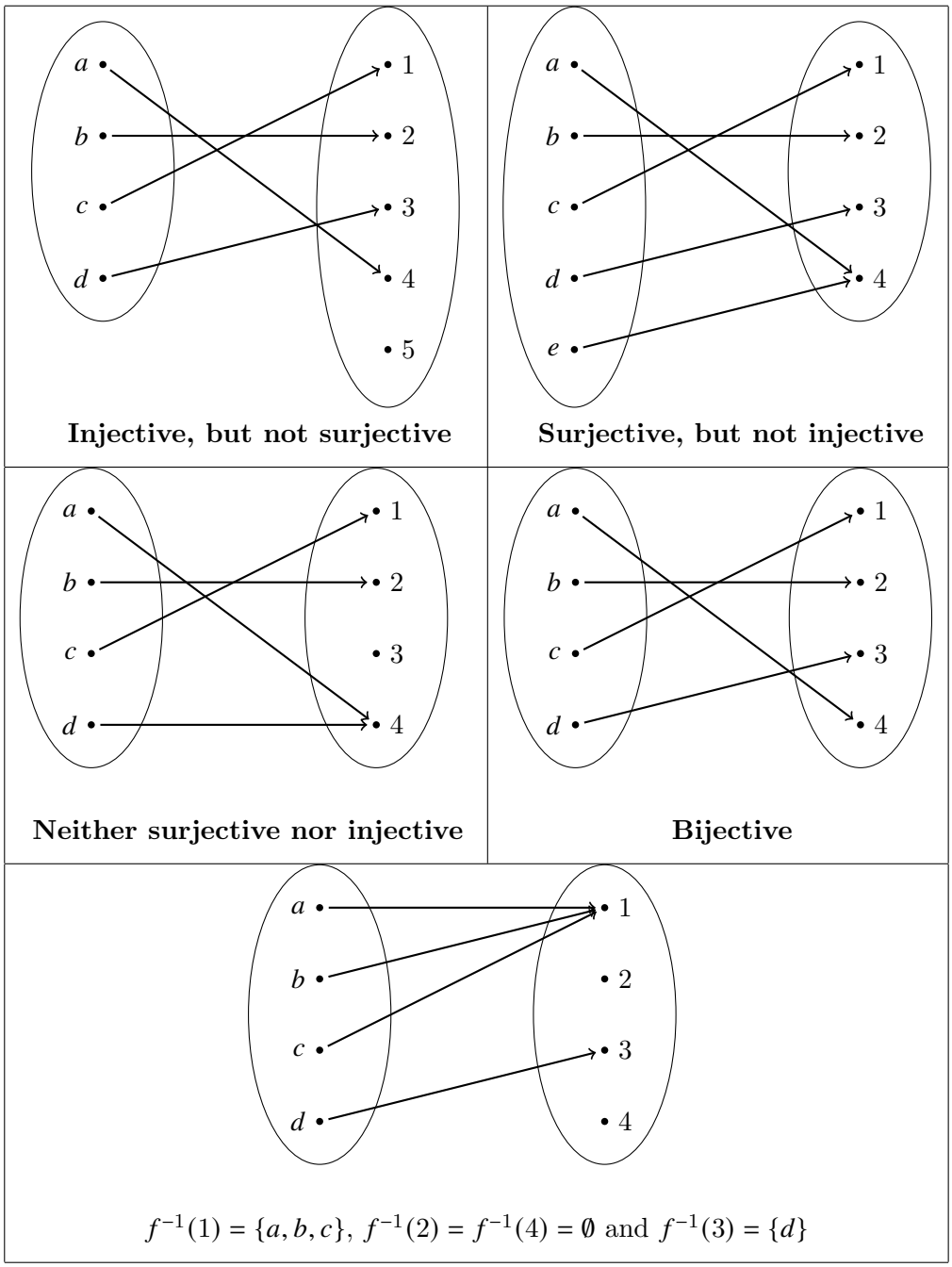


Figure 1: Illustration of injective, surjective and bijective functions and inverse image.

Definition 5.7 (Inverse)**.** A function $f : S \to T$ is said to be invertible if there exists an function $g : T \to S$ such that $g \circ f = \mathbb{I}_S$ and $f \circ G = \mathbb{I}_T$.

In the definition, g is called inverse of f, that is $g = f^{-1}$ and vice verse. Always remember that g is the inverse of f w.r.t composition of functions. You might wonder why do we consider two conditions $g \circ f = \mathbb{I}_S$ and $f \circ g = \mathbb{I}_T$? Why not consider only one of them? Look at the following example. Let $S = \{1\}$ and $T = \{1, 2\}$. Let $f : S \to T$ and $g : T \to S$ be defined as $f(1) = 1$ and $g(1) = g(2) = 1$. Now, check that $g \circ f = \mathbb{I}_S$, in fact, $g(f(1)) = 1$. But, $f \circ g \neq \mathbb{I}_T$ because $f(g(2)) = 1 \neq 2$.

Example 5.12. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 3x + 1$ for $x \in \mathbb{R}$. Then the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(y) = (y - 1)/3$ for $y \in \mathbb{R}$ is the inverse of f. In fact, $g(f(x)) = g(3x + 1) = x \ \forall x \in \mathbb{R}$. Similarly, $f(g(y)) = y \ \forall y \in \mathbb{R}$.

Lemma 5.3. *A function $f : S \to T$ is bijective iff it is invertible.*

Proof. Exercise. □

Exercise 5.13. Find the inverses of the functions defined in Examples 5.5 and 5.6.

Lemma 5.4. *Let $f : S \to T$, where S and T are nonempty finite sets. Then, prove the following statements.*

1. *f is one-one $\implies |S| \leq |T|$.*
2. *f is onto $\implies |T| \leq |S|$.*
3. *f is one-one and $|S| = |T| \implies f$ is bijection.*
4. *f is onto and $|S| = |T| \implies f$ is bijection.*

Proof. Exercise. Note that items 1 and 2 are also true for any sets (not necessarily finite). □

5.2 Countable and Uncountable Sets

Definition 5.8. A set S is said to be *countably infinite*, if there is a bijective function[4] from $\mathbb{N}$ to S. A set S is *countable*, if either S is *finite* or *countably infinite*. If a set S is not countable, we say A is *uncountable*.

By definition, any finite set is countable. $\mathbb{N}$ is countable as $\mathbb{I}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ is a bijection. Based on the bijection defined in Example 5.6, $\mathbb{Z}$ is countable. One can check that set of odd (resp. even) positive integers is countable. What can be said about $\mathbb{Q}$? Note that a set A is countably infinite means, elements of the set can enumerated as $A = \{a_1, a_2, \ldots, \} = \{a_n : n \in \mathbb{N}\}$.

Lemma 5.5. *Union of a finite set and a countably infinite set is countable.*

Proof. Let A be a finite set and B be a countably infinite set. W.l.o.g, we can write $A = \{a_1, a_2, \ldots, a_k\}$ for some positive integer k and $B = \{b_n : n \in \mathbb{N}\}$. We have to define a bijective function $f : \mathbb{N} \to A \cup B$. In fact, the following function

$$f(n) = \begin{cases} a_n & \text{if } n \leq k \\ b_{n-k} & \text{otherwise} \end{cases}$$

is a bijection. □

Lemma 5.6. *Union of two countable sets is countable.*

Proof. Let S_1 and S_2 be two countable sets. If any one of S_1 and S_2 is finite, then the proof is obvious. So, we can assume that S_1 and S_2 are countably infinite. Then we can write $S_1 = \{x_n : n \in \mathbb{N}\}$ and $S_2 = \{y_n : n \in \mathbb{N}\}$. We have to show a bijection $f : \mathbb{N} \to S_1 \cup S_2$. In fact, the following function

$$f(n) = \begin{cases} y_{n/2} & \text{if } n \text{ is even} \\ x_{(n+1)/2} & \text{if } n \text{ is odd} \end{cases}$$

is a bijection. □

[4] This is also known as enumeration.

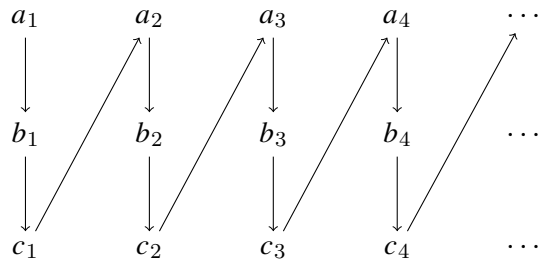
Corollary 5.7. *Union of any finite number of countable sets is countable.*

Proof. Follows induction 4.1 and Lemma 5.6. □

Graph-Theoretic Visualization. Let A, B and C be three countable sets. So, we can write $A = \{a_n : n \in \mathbb{N}\}$, $B = \{b_n : n \in \mathbb{N}\}$ and $C = \{c_n : n \in \mathbb{N}\}$. We have to show that $S = A \cup B \cup C$ is countable set. It suffices to show numbering all the elements of S. In fact, $S = \{a_1, b_1, c_1, a_2, b_2, c_2, a_3, \ldots, \}$. More precisely, $f : \mathbb{N} \to S$ defined by

$$f(n) = \begin{cases} a_{\lceil n/3 \rceil} & \text{if } n\%3 = 1 \\ b_{\lceil n/3 \rceil} & \text{if } n\%3 = 2 \\ c_{\lceil n/3 \rceil} & \text{if } n\%3 = 0, \end{cases}$$

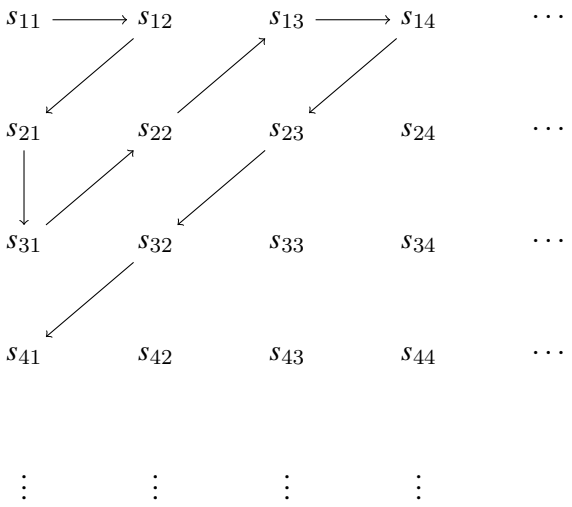
is a bijection. One can visualize the function through the following diagram.



Similarly, by extending the above map one can handle a finite number of countable sets.

Lemma 5.8. *Countable union of countable sets is countable.*

Proof. We have to show that $S = \bigcup_{i \in \mathbb{N}} S_i$ is countable. W.l.o.g, we can assume that all S_i's are countably infinite. So, we can write $S_i = \{s_{ij} : j \in \mathbb{N}\}$ for any $i \in \mathbb{N}$. In the following, we list out all elements of S together with a zigzag path.



The above path essentially gives an enumeration of S. In fact, the bijection $f : \mathbb{N} \to S$ works as follows: $f(1) = s_{11}, f(2) = 12, f(3) = s_{21}, f(4) = s_{31}, f(5) = s_{22}, f(6) = s_{13}$, and so on. □

Corollary 5.9. $\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}$ *(finite product) is countable.*

Proof. Hint: First show that $\mathbb{N} \times \mathbb{N}$ is countable, then apply mathematical induction. □

Corollary 5.10. $\mathbb{Q}$ *is countable.*

Proof. Let us define $\mathbb{Q}^+ = \{x \in \mathbb{Q} : \ x > 0\}$ and $\mathbb{Q}^- = \{x \in \mathbb{Q} : \ x < 0\}$. Note that $\mathbb{Q}^+$ can be written as $\mathbb{Q}^+ = \bigcup_{i \in \mathbb{N}} Q_i$, where $\mathbb{Q}_i = \{i/q : q \in \mathbb{N}\}$. Since each $\mathbb{Q}_i$ is countable, so is $\mathbb{Q}^+$ thanks to Lemma 5.8. Similarly, $\mathbb{Q}^-$ is countable. Therefore, $\mathbb{Q} = \mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$ is countable. □

6 Combinatorics

In this section, we discuss four fundamental concepts of permutation and combination.

Case 1: Permutation. Given a set of n objects, pick r objects and arrange them in order. Each arrangement is called a permutation. The number of all such arrangements is denoted by $P(n, r)$. It can be calculated as follows.

$$\begin{aligned} P(n,r) &= \underset{(1\text{st})}{n} \times \underset{(2\text{nd})}{(n-1)} \times \underset{(3\text{rd})}{(n-2)} \times \ldots \times \underset{(\text{r-th})}{(n-(r-1))} \\ &= \frac{n!}{(n-r)!}. \end{aligned}$$

So, $p(n, n) = n!$.

Exercise 6.1. What is the number injective functions from a set of size r to a set of size n?

Exercise 6.2. What is the number bijective functions from a set of size n to a set of size n?

Case 2: Combination. Given a set of n objects, select r objects out of it (that is, order does not matter). One such selection is called a combination. The number ways such selection can be done is denoted by $C(n, r)$ or $\binom{n}{r}$. Then we can write $P(n, r) = C(n, r) \cdot r!$, because a particular selection can be arranged in $r!$ many ways. So, $\binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r! \cdot (n-r)!}$.

Problem 6.3. Prove that $\binom{n}{r} = \binom{n}{n-r}$.

Proof.

$$\binom{n}{r} = \frac{n!}{r! \cdot (n-r)!} = \frac{n!}{\cdot (n-r)! \cdot (n-(n-r))!} = \binom{n}{n-r}.$$

□

Problem 6.4. Show that $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$.

Proof. Let $*$ be any object out of these n objects. Then, r objects can be selected either including $*$ or excluding $*$. In fist case, r objects can be selected in $\binom{n-1}{r-1}$ many ways, whereas in the second case, it can be done $\binom{n-1}{r}$ many ways. How? So, $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$. □

Problem 6.5. Find the number of identifiers of length at most 4. Assume that an identifier always starts with a letter and consists of letters and digits only.

Ans. The answer is $\underset{\text{(length 1)}}{52} \times \underset{\text{(length 2)}}{52 \times 62} + \underset{\text{(length 3)}}{52 \times 62 \times 62} + \underset{\text{(length 4)}}{52 \times 62 \times 62 \times 62}$. □

Problem 6.6. There are 3 Russians, 4 Koreans and 5 Germans. How many ways one can select two people with different nationalities?

Ans.

- Two people can be chosen from 3 Russians and 4 Koreans with different nationalities in $\binom{3}{1} \times \binom{4}{1}$ many ways.
- Two people can be chosen from 4 Koreans and 5 Germans with different nationalities in $\binom{4}{1} \times \binom{5}{1}$ many ways.
- Two people can be chosen from 5 Germans and 3 Russians with different nationalities is $\binom{5}{1} \times \binom{3}{1}$ many ways.

So, the answer is $\binom{3}{1} \times \binom{4}{1} + \binom{4}{1} \times \binom{5}{1} + \binom{5}{1} \times \binom{3}{1}$. □

Problem 6.7. Show that $|\{0,1\}^n| = 2^n$.

Ans. Basically, we have to count the number of n-bit strings over $\{0,1\}$.

- **Using cartesian product.** $\{0,1\}^n = \{0,1\} \times \cdots \times \{0,1\}$ (n-times)
- **Using product rule.** There are n positions and two options, 0 and 1 for each position. So, each position can be filled up two ways. Therefore, the number of n-bit strings is $2 \times \cdots \times 2$ (n-times) $= 2^n$.
- **Using Binomial.** Look, a string can have either n number of 1's, or $(n-1)$ number of 1's or ... or a single 1 or no 1's. The number of strings with exactly i number of 1's is $\binom{n}{i}$. How? Therefore,

$$|\{0,1\}^n| = \underset{\text{no 1's}}{\binom{n}{0}} + \underset{\text{singe 1}}{\binom{n}{1}} + \underset{\text{2 1's}}{\binom{n}{2}} + \cdots + \underset{\text{n 1's}}{\binom{n}{n}} = \underset{\text{(how?)}}{(1+1)^n} = 2^n.$$

□

Remark 6.8. Any of the above approaches can be applied to calculate $|\mathcal{P}(A)|$, where A is a finite set.

Case 3: Permutation with repetition. What is the number of arrangements of r objects out of n given objects, where *repetition* of the objects are allowed? The fist object will have n choices, the 2nd object will have n choices (because of repetition), the 3rd object will have n choices (because of repetition) and so on. So, the total number of arrangements with repetition is $n \times \cdots \times n$ (r-times) $= n^r$. This is also know as product rule.

Exercise 6.9. Let X and Y be two non-empty sets. Let the notation Y^X denote the set of all functions X to Y. Then, calculate $|Y^X|$. The notation Y^X carries some meaning. Can you identify that meaning?

Case 4: Combination with repetition. What is the number of selections of r objects out of n objects, where *repetition* is allowed?

OR

How many ways r objects can be selected from n categories of objects, where from each category any number of objects can be chosen?

Ans. Note that there is no restriction on r and n, that is, either $n \geq r$ or $n \leq r$. The answer is $\binom{r+n-1}{n-1}$. The explanation is given by the concept of bar (|) and cross (X). Note that the bars basically separate the categories. Since there are n categories (or n objects with repetition), $(n-1)$ bars are sufficient to categorically group them. A cross represents a particular object of some category. Basically, we have to select $(n-1)$ positions for the bars out of $(r+n-1)$ positions and all remaining positions will be filled with crosses. For ease of explanation, let $r = 6$ and $n = 4$. Let the objects/categories be denoted by a_1, a_2, a_3 and a_4. So, out of $6+4-1 = 9$ (total no. of bars and crosses) positions, we have to select $(n-1) = 3$ positions for the bars. How does this work? A selection goes like this, the first category objects (a_1) followed the first bar, the second category objects (a_2) followed by the second bar, and so on. For example, if one selects position 1, 3 and 5 for the bars, then the selection will be of the following form:

$$\underset{1}{|}\underset{2}{X}\underset{3}{|}\underset{4}{X}\underset{5}{|}\underset{6}{X}\underset{7}{X}\underset{8}{X}\underset{9}{X} \implies \underset{1}{|}\underset{2}{a_2}\underset{3}{|}\underset{4}{a_3}\underset{5}{|}\underset{6}{a_4}\underset{7}{a_4}\underset{8}{a_4}\underset{9}{a_4}.$$

As we can see the first bar separates the first and the second categories of objects, whereas as the 2nd bar does for the 2nd and the 3rd categories of objects and so on. Since the fist bar is placed at position one, no a_1's appear in the selection.

If one chooses the positions 3, 5 and 7 for the bars, then the selection has the following from:

$$\underset{1}{X}\underset{2}{X}\underset{3}{|}\underset{4}{X}\underset{5}{|}\underset{6}{X}\underset{7}{|}\underset{8}{X}\underset{9}{X} \implies \underset{1}{a_1}\underset{2}{a_1}\underset{3}{|}\underset{4}{a_2}\underset{5}{|}\underset{6}{a_3}\underset{7}{|}\underset{8}{a_4}\underset{9}{a_4}.$$

If one chooses the positions 3, 5 and 6 for the bars, then the selection has the following from:

$$\underset{1}{X}\underset{2}{X}\underset{3}{|}\underset{4}{X}\underset{5}{|}\underset{6}{|}\underset{7}{X}\underset{8}{X}\underset{9}{X} \implies \underset{1}{a_1}\underset{2}{a_1}\underset{3}{|}\underset{4}{a_2}\underset{5}{|}\underset{6}{|}\underset{7}{a_4}\underset{8}{a_4}\underset{9}{a_4}.$$

□

Problem 6.10. What is the number of selections of r objects out of n objects, where *repetition* is allowed and each object should appear at least once?

OR

How many ways r objects can be selected from n categories of objects, where any number of objects can be chosen from each category and at least one object should appear from each category?

Ans. In this case, we have $n \leq r$. The answer is $\binom{r-n+n-1}{n-1} = \binom{r-1}{n-1}$. (Why?) □

Exercise 6.11. Let V be a set of n vertices. How many graphs can be constructed using V as vertex set? Assume that self loops are not allowed.

Exercise 6.12. Let A be a set with $|V| = n$. How many binary relations on A can be defined? How many binary relations on A are reflexive? How many binary relations on A are symmetric?

Sampling Problem. We have discussed four cases of selection/arrangement problems. All these cases can be viewed through sampling problem. Sample r things out of n things under the following constraints.

- Order matters (A)
- With replacement (B)

When A is 'yes', this is the case of arrangement, otherwise it is the case of selection. When B is 'true', it is the case of sampling with replacement (or repetition), otherwise, it is sampling without replacement. The number of ways sampling are possible is given in the 3rd column of the following table:

A	B	#	Remarks
Yes	Yes	n^r	**Case 3**
Yes	No	$P(n,r)$	**Case 1**
No	Yes	$\binom{r+n-1}{n-1}$	**Case 4**
No	No	$\binom{n}{r}$	**Case 2**

Exercise 6.13. Let n and r be positive integers. Consider the following problems related to n-variables polynomial.

1. How many monomials of degree at most r is possible under following two constraints:
   (a) order of the variables matters.
   (b) order of the variable does not matter.
2. How many ways a zero polynomial in n variables can be expressed, where the degree of any monomial can be at most r?
3. How many distinct multivariate polynomials over $\{0,1\}$ in n variables are possible, where the degree of any monomial can be at most r?

7 Basic Notations and Operations of Languages

An alphabet, typically denoted by Σ, is a finite, nonempty set of symbols. Let $\emptyset$ and ϵ denote empty set and empty string respectively[5]. The set of all finite strings over Σ is denoted bt Σ^*. So, we can write

$$\Sigma^* = \cup_{i=0}^{\infty} \Sigma_i,$$

where Σ_i denotes the set of all strings over Σ of length i.

Exercise 7.1. What is the cardinality of Σ^*?

A language L over Σ is defined to be a subset of Σ^*, that is, some collection of strings over Σ. Note that $\emptyset$ represents an empty language, whereas $L = \{\epsilon\}$ is a language consisting of empty string ϵ. For $L_1, L_2 \subseteq \Sigma^*$, we define the following operations:

- (**Union**). $L_1 \cup L_2 = \{\omega \in \Sigma^* : \ \omega \in L_1 \text{ or } \omega \in L_2\}$.
  For example, let $\Sigma = \{0,1\}$, $L_1 = \{00, 11\}$ and $L_2 = \{1, 00, 111\}$, then $L_1 \cup L_2 = \{1, 00, 11, 111\}$.
- (**Concatenation**). $L_1L_2 = \{\omega_1\omega_2 \in \Sigma^* : \ \omega_1 \in L_1 \text{ and } \omega_2 \in L_2\}$.
  For example, let $\Sigma = \{0,1\}$, $L_1 = \{00, 11\}$ and $L_2 = \{1, 00, 111\}$, then $L_1L_2 = \{001, 111, 0000, 1100, 00111, 11111\}$.
- (**Kleene star**). For a language L over Σ, the *Kleene star*, denoted by L^*, is defined as follows: $L_0 = \{\epsilon\}$, $L_1 = L$, $L_{n+1} = L_nL_1$ and $L^* = \cup_{n=0}^{\infty} L_n$. Note that L^* is also called the *Kleene star* or *Kleene closure*[6] of L.

[5]The distinction between $\emptyset$ and ϵ is that the former one is a set without having any element, whereas the latter one is a string without having any symbol

[6]The name was given after Stephen Cole Kleene, a founder of the branch of mathematical logic.

- $L^+ = L^* \setminus \{\epsilon\}$.
- (**Reversal**). For a string $\omega = \omega_1\omega_2\cdots\omega_{n-1}\omega_n$, where $\omega_i \in \Sigma^*$, its reverse string is defined to be $\omega^r = \omega_n\omega_{n-1}\cdots\omega_2\omega_1$. For a language $L \subseteq \Sigma^*$, its reversal language, denoted by L^r, is defined as $L^r = \{\omega^r : \omega \in L\}$. For example, if $L = \{10, 0011, 110, 111\}$, then its reversal is $L^r = \{01, 1100, 011, 111\}$.

Remark 7.2. For any language L, $\emptyset L = \emptyset = L\emptyset$ and $\{\epsilon\}L = L = L\{\epsilon\}$. Also $\emptyset^* = \{\epsilon\}$.

Exercise 7.3. Prove or disprove $|L_1L_2| = |L_1| \cdot |L_2|$ for any two languages L_1 and L_2.

The following result is very important and will be proved in module-4 using *diagonalization* method.

Theorem 7.1 (Cantor)**.** $2^{\mathbb{N}}$ *is uncountable.*

Question. How many languages over a finite alphabet Σ are possible?

Exercise 7.4. How many infinite sequences over $\{0, 1\}$ are possible.