Discrete Mathematics and Algorithms (CSE611)

Dr. Ashok Kumar Das

Assistant Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad
Gachibowli 500 032, Hyderabad, India

E-mail: *ashok.das@iiit.ac.in*
Homepage: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Homepage: https://sites.google.com/site/iitkgpakdas/

Topic: **Set Theory**

SET THEORY

- A set is a well-defined collection of *distinct* objects, which are called members of the set or elements of the set.
- **Representation of a set**
  - **Tabular form:** If the set A consists of the elements 1, 2, 3, and 4, then we express the set in the “tabular form” as $A = \{1, 2, 3, 4\}$.
  - **Set-builder form:** A set is expressed in this form by displaying a typical element and by stating the properties which the elements of the set must satisfy.
    The symbol $A = \{x | P(x)\}$ or
    $A = \{x : P(x)\}$
    states that A is a set of elements x which satisfy the condition $P(x)$; the symbol ‘:’ or ‘$|$’ is read as ‘such that’.

- **Examples**

$$
\begin{aligned}
A &= \{1, 3, 5, \ldots, 39\} && (1)\\
&= \{x | x \text{ is a positive odd integer} < 40\}.\\
B &= \{2, 4, 6, \ldots\} && (2)\\
&= \{x | x = 2n, n \text{ being a natural number}\}.\\
X &= \{1, 8, 27, 64, \ldots\} && (3)\\
&= \{x | x = n^3, n \text{ being a positive integer}\}.\\
S &= \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} && (4)\\
&= \{x | x = 5n, n \text{ is an integer}\}.
\end{aligned}
$$

- **Null Set:** A set, having no elements, is defined as the null set or the empty set. An empty set is denoted by ϕ.
- **Finite Set:** A set is finite, if it be empty or contains a finite number of elements.
- **Infinite Set:** A set contains an infinite number of elements is called an infinite set.
  Example: The set $\{1, 2, 3, 4, 5\}$ is a finite set and the set $\{x_1, x_2, x_3, \ldots\}$ is an infinite set.
- **Order of a set:** The number of elements of a finite set A is called the order or cardinal number or cardinality of the set A and is symbolically denoted by $n(A)$ or $|A|$.
  Example 1: If $A = \{1, 2\}$ and $B = \{1, 2, 3\}$, then $|A| = 2$ and $|B| = 3$.
  Example 2: The null set is regarded as a finite set of order zero, that is $|\phi| = 0$.

Notations for some well-known sets

- N the set of all natural numbers
- Z the set of all integers
- Q the set of all rational numbers, r such that $r = \frac{a}{b}$, $a, b \in Z$, with $b \neq 0$ and $\gcd(a, b) = 1$
- R the set of all real numbers
- C the set of all complex numbers $z = a + ib$, $a, b \in R$
- E the set of all even integers
- Z^+, Q^+, R^+ the corresponding sets of positive quantities only
- Z^-, Q^-, R^- the corresponding sets of negative quantities only

- **Sub-set:** If every element of a set A be also an element of another set B, then A is called a subset of B and we write it as $A \subseteq B$. Mathematically, $A \subseteq B$ means if an arbitrary element $x \in A$, then $x \in B$ also.
- **Proper subset:** If, however, the set B contains some elements which are not the elements of a set A, then A is called a proper subset of B and we write it as $A \subset B$.
- **Comparable:** Two sets A and B are said to be comparable, if either $A \subseteq B$ or $B \subseteq A$.
- **Equality of sets:** Two sets A and B are said to be equal, that is $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$.
- **Disjoint set:** Two sets A and B are said to be disjoint, if they have no element in common, that is $A \cap B = \emptyset$.

- **Difference between sets:** The difference between two sets A and B in that order is the set of elements which belong to A, but do not belong to B.
  $A - B$ or $A \setminus B = \{x | x \in A, \text{but}\, x \notin B\}$
  $B - A$ or $B \setminus A = \{x | x \in B, \text{but}\, x \notin A\}$
  Example: Let $A = \{1, 2, 3, 4\}$ and $B = \{5, 2, 3, 6\}$. Then $A - B = \{1, 4\}$ and $B - A = \{5, 6\}$.
- **Theorem:** If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
- **Theorem:** If $A \subseteq B$ and $B \subseteq A$, then $A = B$.
- **Theorem:** The null set $\emptyset$ is a proper subset of every set except $\emptyset$ itself.

- **Power set:** A set formed of all the subsets of a set S as its element is called a power set of S and is symbolically denoted by $\mathcal{P}(S)$.
  Example: If $S = \{a, b, c\}$, then
  $\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.
- *Notes:* (1) The null set $\emptyset$ is an element/member of $\mathcal{P}(S)$.
  (2) The set S being a subset of itself is also an element of the power set $\mathcal{P}(S)$.
- **Theorem:** If a finite set S has n elements, then its power set $\mathcal{P}(S)$ has 2^n elements. In other words, $|\mathcal{P}(S)| = 2^{|S|}$.
- **Quiz.** What will happen for the power set $\mathcal{P}(S)$, if S is itself a null set?

- **Universal set:** A universal set, U is the set of elements from which elements may be chosen to form sets for a particular discussion.
  Example: The set of even numbers is a subset of the universal set of whole numbers.
- **Complement of a set:** Let S be a given subset of the universal set U. The complement of S relative to U is the set of all elements of U which are not elements of S, and it is denoted by $\sim S$ or S' or S^c or $\overline{S}$.
  Example: If $U = \{1, 2, 3, 4, 5, 6\}$ and $S = \{2, 3, 4\}$, then $S' = \{1, 5, 6\}$.
  Symbolically, $S' = \{x | x \in U \text{ and } x \notin S\}$.

Venn-Euler diagram

- It is a schematic representation of sets by certain areas containing the elements of the sets, being represented by the points of the respective areas.

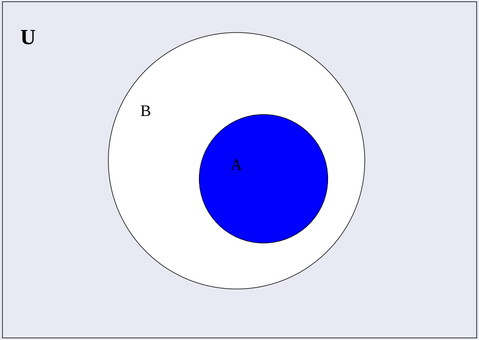

Figure: $A \subseteq B$

Venn-Euler diagram

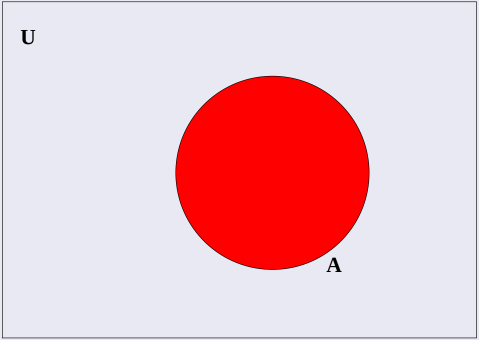

Figure: $A' = U - A$

Basic Set Operations

- **Union or Join** The union of two sets A and B is denoted and defined by

$$\begin{aligned} A \cup B &= \{x | x \in A \text{ or } x \in B\} \\ &= \{x | x \in A \vee x \in B\}. \end{aligned}$$

- If $A_1, A_2, \ldots, A_n$ be the subsets of X, where n is a positive integer, then

$$\begin{aligned} A_1 \cup A_2 \cup \ldots \cup A_n &= \cup_{i=1}^{n} A_i \\ &= \{x | x \in A_i \text{ for some value } i, 1 \leq i \leq n\}. \end{aligned}$$

- Example: If $A = \{1, 2, 3\}$ and $B = \{4, 3, 5, 6\}$, then $A \cup B = \{1, 2, 3, 4, 5, 6\}$.

Basic Set Operations (Continued...)

- From the Venn diagram, it is easy to observe the following theorems.
  1. $A \cup A = A$
  2. $A \cup U = U$
  3. If $A \subseteq B$, then $A \cup B = B$
  4. $A \cup B = B \cup A$
  5. $A \cup \emptyset = A$
  6. $A \cup A' = U$

Basic Set Operations (Continued...)

- **Intersection or Meet** The intersection of two sets A and B is denoted and defined by

$$\begin{aligned} A \cap B &= \{x | x \in A \,\text{and}\, x \in B\} \\ &= \{x | x \in A \wedge x \in B\}. \end{aligned}$$

- If $A_1, A_2, \ldots, A_n$ be the subsets of X, where n is a positive integer, then

$$\begin{aligned} A_1 \cap A_2 \cap \ldots \cap A_n &= \cap_{i=1}^{n} A_i \\ &= \{x | x \in A_i, \forall i, 1 \leq i \leq n\}. \end{aligned}$$

- Example: If $A = \{a, b, c\}$ and $B = \{c, d, e\}$, then $A \cap B = \{c\}$.

Basic Set Operations (Continued...)

- From the Venn diagram, the following theorems are obvious:
  1. $A \cap A = A$
  2. $A \cap U = A$
  3. If $A \subseteq B$, then $A \cap B = A$
  4. $A \cap B = B \cap A$
  5. $A \cap \emptyset = \emptyset$
  6. $A \cap A' = \emptyset$

Laws of Algebra on Sets

Let A, B and C be three any sets.

- **Commutative laws**
  1. $A \cup B = B \cup A$
  2. $A \cap B = B \cap A$
- **Associative laws**
  1. $A \cup (B \cup C) = (A \cup B) \cup C$
  2. $A \cap (B \cap C) = (A \cap B) \cap C$
- **Idempotent laws**
  1. $A \cup A = A$
  2. $A \cap A = A$

Laws of Algebra on Sets (Continued...)

Let A, B and C be three any sets.

- **Distributive laws**
  1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- **De Morgon's laws**
  1. $A - B = A \cap B'$
  2. $(A \cup B)' = A' \cap B'$
  3. $(A \cap B)' = A' \cup B'$
  4. $A - (B \cup C) = (A - B) \cap (A - C)$
  5. $A - (B \cap C) = (A - B) \cup (A - C)$

Symmetric Difference

Let A and B be two sets.

- The symmetric difference of A and B is denoted and defined by

$$\begin{aligned} A \triangle B &= (A - B) \cup (B - A) \\ &= \{x \mid [x \in A \text{ and } x \notin B] \text{ or } [x \in B \text{ and } x \notin A]\}. \end{aligned}$$

- Example: If $A = \{1, 2, 4, 7, 9\}$ and $B = \{2, 3, 7, 8, 9\}$, then $A - B = \{1, 4\}$, $B - A = \{3, 8\}$.
  Thus, $A \triangle B = \{1, 4\} \cup \{3, 8\} = \{1, 3, 4, 8\}$.
- It can be easily verified that
  (i) $A \triangle \emptyset = A$,
  (ii) $A \triangle A = \emptyset$,
  (iii) $A \triangle B = \emptyset \Rightarrow A = B$.

Cartesian product of sets

- The Cartesian product of two sets A and B is denoted and defined by

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

More generally, the Cartesian product of n sets A_1, A_2, . . ., A_n is

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_i \in A_i, 1 \leq i \leq n\}.$$

- Example: If $A = \{a, b, c\}$ and $B = \{m, n\}$, then $A \times B = \{(a, m), (a, n), (b, m), (b, n), (c, m), (c, n)\}$.
- It can be easily verified that if $|A| = m$ and $|B| = n$, then $|A \times B| = mn$.
- In general, $A \times B \neq B \times A$.

The Inclusion-Exclusion Principle

- Let $A_1, A_2, \ldots, A_n$ be n finite sets. Then

$$\begin{aligned} |\cup_{i=1}^{n} A_i| &= \sum_{i=1}^{n} |A_i| - \sum_{i,j=1; i\neq j}^{n} |A_i \cap A_j| \\ &+ \sum_{i,j,k=1; i\neq j\neq k}^{n} |A_i \cap A_j \cap A_k| - \ldots \\ &+ (-1)^{n+1} |\cap_{i=1}^{n} A_i| \end{aligned}$$

- Special cases
  - When $n = 2$, $|A \cup B| = |A| + |B| - |A \cap B|$
  - When $n = 3$, $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$

Problem: Prove that $(A - B)$, $(B - A)$ and $A \cap B$ are disjoint, where A and B are two sets.

Two sets X and Y are disjoint, if $X \cap Y = \emptyset$.
Now,

$$\begin{aligned}
(A - B) \cap (A \cap B) &= (A \cap B') \cap (A \cap B), \text{by De Morgan's laws} \\
&= (A \cap B') \cap (B \cap A), \text{by Commutative laws} \\
&= A \cap (B' \cap B) \cap A, \text{by Associative laws} \\
&= A \cap (\emptyset \cap A) \\
&= A \cap \emptyset \\
&= \emptyset
\end{aligned}$$

Similarly, it can be shown that
$(B - A) \cap (A \cap B) = \emptyset$
$(A - B) \cap (B - A) = \emptyset$

Problem

- The number of elements in a finite set S is denoted by $|S|$.
  (a) Starting from the fact that $|A \cup B| = |A| + |B|$ when A and B are two disjoint sets, show that in general, $|A \cup B| = |A| + |B| - |A \cap B|$.
  (b) For any three sets A, B, and C, show that
  $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$.

Problem [The Inclusion-Exclusion Principle]: Find the number of positive integers ≤ 2076 and divisible by neither 4 nor 5.

Let $A = \{x \in N | x \leq 2076 \text{ and divisible by } 4\}$, and
$B = \{x \in N | x \leq 2076 \text{ and divisible by } 5\}$.
By the Inclusion-Exclusion Principle, we have,

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ &= \lfloor \frac{2076}{4} \rfloor + \lfloor \frac{2076}{5} \rfloor - \lfloor \frac{2076}{4 \times 5} \rfloor \\ &= 519 + 415 - 103 \\ &= 831. \end{aligned}$$

Thus, among the first 2076 positive numbers, there are $2076 - 831 = 1245$ integers NOT divisible by neither 4 nor 5.

A Number-Theoretic Function

- An integer $p(> 1)$ is called a prime number or simply a prime, if its only positive divisors are 1 and itself. In other words, p does not have any non-trivial divisor d such that $1 < d < p$.
- Let x be a positive real number. Then $\pi(x)$ denotes the number of primes $\leq x$.
- **Prime Number Theorem:** $\pi(x) \to \frac{x}{ln(x)}$ as $x \to \infty$
- **Theorem:** Let $p_1, p_2, \ldots, p_t$ be the primes $\leq \sqrt{n}$. Then $\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \lfloor \frac{n}{p_i} \rfloor + \sum_{i<j} \lfloor \frac{n}{p_i p_j} \rfloor - \sum_{i<j<k} \lfloor \frac{n}{p_i p_j p_k} \rfloor + \ldots + (-1)^t \lfloor \frac{n}{p_1 p_2 \ldots p_t} \rfloor$

Problem: Find the number of primes ≤ 100.

Here $n = 100$. Then $\pi(\sqrt{n}) = \pi(\sqrt{100}) = \pi(10) = 4$. The four primes $\leq \sqrt{n} = 10$ are $2, 3, 5$ and 7. Let $p_1 = 2, p_2 = 3, p_3 = 5$ and $p_4 = 7$, $t = 4$. From the previous theorem, we have,

$$\begin{aligned}
\pi(100) &= 100 - 1 + 4 - (\lfloor\frac{100}{2}\rfloor + \lfloor\frac{100}{3}\rfloor + \lfloor\frac{100}{5}\rfloor + \lfloor\frac{100}{7}\rfloor) \\
&\quad +(\lfloor\frac{100}{2.3}\rfloor + \lfloor\frac{100}{2.5}\rfloor + \lfloor\frac{100}{2.7}\rfloor + \lfloor\frac{100}{3.5}\rfloor + \lfloor\frac{100}{3.7}\rfloor + \lfloor\frac{100}{5.7}\rfloor) \\
&\quad -(\lfloor\frac{100}{2.3.5}\rfloor + \lfloor\frac{100}{2.3.7}\rfloor + \lfloor\frac{100}{2.5.7}\rfloor + \lfloor\frac{100}{3.5.7}\rfloor) + \lfloor\frac{100}{2.3.5.7}\rfloor \\
&= 103 - (50 + 33 + 20 + 14) + (16 + 10 + 7 + 6 + 4 + 2) \\
&\quad -(3 + 2 + 1 + 0) + 0 \\
&= 25.
\end{aligned}$$

This result is consistent with the sieve of Eratosthenes.

Quiz: Find the number of primes in between 50 and 100.

Solution

- Step 1. Find the number of primes ≤ 50. We have $\pi(50) = 15$.
- Step 2. Find the number of primes ≤ 100. We have $\pi(100) = 25$.
- Step 3. Finally, calculate the number of primes ≥ 50 and ≤ 100, which is $\pi(100) - \pi(50) = 25 - 15 = 10$.

This is cinsistent with the sieve of Eratothenes.
Note: Using the sieve of Eratothenes, the primes ≤ 100 are:
$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,$
$53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Problem: If $A = \{1, 2\}$, $B = \{2, 3\}$ and $C = \{3, 4\}$, then find $A \times (B \cup C)$. Further verifies whether $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Part 1: We have, $B \cup C = \{2, 3, 4\}$.
Now,

$$\begin{aligned} A \times (B \cup C) &= \{1, 2\} \times \{2, 3, 4\} \\ &= \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\} \end{aligned}$$

Part 2: We also have,

$$\begin{aligned} (A \times B) \cup (A \times C) &= \{(1, 2), (1, 3), (2, 2), (2, 3)\} \\ &\quad \cup \{(1, 3), (1, 4), (2, 3), (2, 4)\} \\ &= \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\} \\ &= A \times (B \cup C) \end{aligned}$$

Problem: Let X, A and B be three sets such that $X \cap A = X \cap B$ and $X \cup A = X \cup B$. Prove that $A = B$.

We have to prove $A \subseteq B$ and $B \subseteq A$.
Let $x \in A$.
We have then two cases:

- Case 1: Let $x \in X$.
  Then $x \in A \cap X = X \cap B$.
  Thus, $x \in B$.
- Case 2: Let $x \notin X$.
  Then $x \in A$
  $\Rightarrow x \in A \cup X = X \cup B$.
  Thus, $x \in B$, since $x \notin X$.
  Hence, for each case, we have $x \in A$
  $\Rightarrow x \in B$.
  As a result, $A \subseteq B$.
  Similarly, one can prove that $B \subseteq A$.

Problem: For any two sets A and B, prove that $A \cap B = A$ if and only if $A \subseteq B$.

We first prove that $A \cap B = A \Rightarrow A \subseteq B$.
Since $A \cap B \subseteq B$ by definition, $A \subseteq B$.
Conversely, we prove that $A \subseteq B \Rightarrow A \cap B = A$.
By definition, $A \cap B \subseteq A$.
If $x \in A$, then $x \in B$, since $A \subseteq B$.
Hence, $x \in A \cap B$ and $A \subseteq A \cap B$.
Thus, $A \cap B = A$.

End of this lecture