Mathematical Preliminaries

Sets:

- An unordered collection of elements (order doesn't matter).
- Can be finite, $\{2, 3, 4\}$, or infinite $\{1, 2, 3, 4...\}$.
- Set **membership**: $\in, \notin$

  Ex: $4 \in \{2, 3, 4\}$, $1 \notin \{2, 3, 4\}$,
- Sets can contain other sets: $\{2, \{5\}\}$, $\{\{0\}\} \neq \{0\} \neq 0$
- Two sets are equal if they contain the same elements.

Common Sets

- Naturals: $N = \{0, 1, 2, 3, 4, ...\}$
- Integers: $Z = \{... - 2, -1, 0, 1, 2, ...\}$
- Rationals: $Q = \{\frac{a}{b} \; | a, b \in Z, b \neq 0\}$
- Reals: R
- Empty set: $\emptyset = \{\}$
- Set **definition**: $'|'$ means "such that".

  Ex: $\{k | k \in N, 0 < k < 4\}$

Set operations

- Subset: $\subseteq$, $\subset$.
- $\forall S, \varnothing \subseteq S$.
- $\forall S, S \subseteq S$.
- Union ($\cup$), Intersection ($\cap$).
- Set **difference**: $S - T = \{x | x \in S \wedge x \notin T\}$.
- Set **complement**: $\neg S$ or $\bar{S} = \{x | x \notin S\} = U - S$, where U is a universal set (everything).
- **Disjoint** sets: $S \cap T = \varnothing$.

Set Cardinality

- **Cardinality**: $|S|$ = number of elements in S.
- **Power set** of a set A, 2^A is the set of all subsets of A.

  Example: $A = \{2, 3\}$, then the power set of A is $2^A = \{\emptyset, \{2\}, \{3\}, \{2, 3\}\}$.

  Question: if $|A| = n$, what is the cardinality of the power set? Answer: 2^n.

- **DeMorgan's laws**:

$$\neg(B \cap C) = \neg B \cup \neg C$$

$$\neg(B \cup C) = \neg B \cap \neg C$$

Cartesian product

- Given two sets A and B, the **Cartesian product** or **cross product** $A \times B$ is the set of all *ordered pairs* wherein the first element is a member of A and the second element is a member of B.

  Example: if $A = \{1, 2\}$ and $B = \{x, y, z\}$, then $A \times B = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}$.

  Question: what is the cardinality of $A \times B$? Answer: $|A| \times |B|$.

Binary relations

- A **binary relation** R on two sets A and B is a subset of the Cartesian product $A \times B$. If $(a, b) \in R$, this is equivalently written as aRb.

- Types of relations $R \subseteq A \times A$:

  - *reflexive*: aRa, for all $a \in A$

  - *symmetric*: $aRb \Rightarrow bRa$, for all $a, b \in A$

  - *transitive*: aRb and $bRc \Rightarrow aRc$, for all $a, b, c \in A$

  - *equivalence*: reflexive and symmetric and transitive.

- Examples: $<$, $\geq$, $=$.

Functions

- A **function** $f : A \to B$ is a binary relation on A and B such that for all $a \in A$, there is one and only one $b \in B$ such that $(a, b) \in f$.

  $(a, b) \in f$ is equivalently written $f(a) = b$.

  A is called $f's$ **domain** and B is the **codomain**.

  We say that a is the **argument** of f and that $f(a) = b$ is the **value (image)** of f at a.

- The **range** of f is the image of its domain, that is, $f(A) = \{b \in B : b = f(a)$ for some $a \in A\}$.

- A function is a **surjection** if its range is its codomain.

Functions (cont'd)

- A function $f : A \to B$ is an **injection (one-to-one)** if distinct arguments to f produce distinct values, that is, if $a \neq a'$ implies $f(a) \neq f(a')$.

  Example:

- A function $f : A \to B$ is a **bijection (one-to-one correspondence)** if it is injective and surjective.

  Example:

Floor, Ceiling

floor and **ceiling**:

- Let $x \in R$, then:
  - $\lfloor x \rfloor =$ largest integer $\leq x$ —"floor". (e.g., $\lfloor 8.2 \rfloor = 8$)
  - $\lceil x \rceil =$ smallest integer $\geq x$ — "ceiling". (e.g., $\lceil 8.2 \rceil = 9$)

  Basic facts:
  - $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$
  - If n is a integer then $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$

$$\lceil \frac{\lceil \frac{n}{2} \rceil}{2} \rceil = \lceil \frac{n}{4} \rceil$$

Polynomial and Exponential

Polynomials:

$$p(n) = \sum_{k=0}^{d} a_k \cdot n^k = a_d \cdot n^d + \ldots a_1 \cdot n + a_0 \tag{1}$$

Exponential Function:

$$a^0 = 1$$
$$a^1 = a$$
$$a^{-1} = 1/a$$
$$(a^m)^n = a^{mn}$$
$$a^m a^n = a^{m+n}$$

Logarithms

Logarithms:

- definitions: $\lg n = \log_2 n$, $\quad \ln n = \log_e n$
- $\log_c ab = \log_c a + \log_c b$.
- $\log_c a^b = b \cdot \log_c a$.
- $\log_c \frac{a}{b} = \log_c a - \log_c b$.
- $\log_c a = \frac{\log_d a}{\log_d c}$. (change base)
- $a^{log_c n} = n^{log_c a}$
- derivatives: $(\ln a)' = \frac{1}{a}$, $\quad (\lg a)' = \frac{\lg e}{a}$.

Factorial

Factorials:

$$n! = \begin{cases} 1 & \text{for } n = 0 \\ n(n-1)! & \text{for } n > 0 \end{cases}$$

Note:

- $n! \leq n^n$
- $\sqrt{2\pi n} \cdot (\frac{n}{e})^n \leq n! \leq \sqrt{2\pi n} \cdot (\frac{n}{e})^{n+(\frac{1}{12}n)}$

The last formula is called "Stirling's approximation" for $n!$.

Summation & Recurrences

Summations

Given a sequence of numbers a_1, a_2, a_3 , ... , a_n , the summation $a_1 + a_2 + \ldots a_n$ is written as

$$\sum_{i=1}^{n} a_i$$

The infinite sum $a_1 + a_2 + \ldots$ is written as

$$\sum_{i=1}^{\infty} a_i$$

and it is formally interpreted as

$$\lim_{n \to \infty} \sum_{i=1}^{n} a_i.$$

General Properties of Summations

Linearity

$$\sum_{k=1}^{n} (ca_k + b_k) = c \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k.$$

Arithmetic Series

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

Sum of squares

$$\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n+1)(2n+1) = \Theta(n^3).$$

Series

Sum of cubes

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4} = \Theta(n^4).$$

Geometric Series For real number $x \neq 1$,

$$\sum_{k=0}^{n} x^k = 1 + x + x^2 + x^3 + \ldots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

The following geometric series are used frequently:

$$\sum_{k=0}^{n} 2^k = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1 - x} \quad \text{(if } |x| < 1\text{)}$$

More Series

Using integrals:

- if f is a continuous, increasing function:

$$\int_{a-1}^{b} f(x)dx \leq \sum_{i=a}^{b} f(i) \leq \int_{a}^{b+1} f(x)dx$$

- if f is a continuous, decreasing function:

$$\int_{a}^{b+1} f(x)dx \leq \sum_{i=a}^{b} f(i) \leq \int_{a-1}^{b} f(x)dx$$

- Example: $f(k) = \frac{1}{k}$

$$ln(n+1) \leq \sum_{i=1}^{n} \frac{1}{k} \leq ln(n) + 1, \qquad \sum_{i=1}^{n} \frac{1}{k} = ln(n) + O(1),$$

Graphs

- A **directed graph** G is a pair (V, E), where V is the set of vertices, and E is the set of edges (i.e. ordered pairs of vertices).

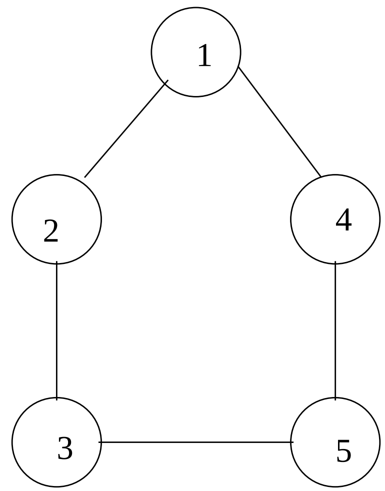
  Review: *adjacency, in-degree, out-degree, path, cycle*.

- In an **undirected graph** $G = (V, E)$, the edges are undordered pairs of vertices.

  Review: *adjacency, degree, path, cycle*.

Review on Graphs

G=(V,E)



$$V = \{1, 2, 3, 4, 5\}$$

$$E = \{(1, 2), (2, 3), (3, 5), (5, 4), (4, 1)\}$$

Representation of graphs

- Adjacency List

- Adjacency Matrix

Review on Trees

- A **free tree** is a connected, acyclic, undirected graph.
- A **rooted tree** is a free tree in which one vertex (the root) is distinguished from the others.

  Review: *ancestor/descendant, parent/child, siblings, external/internal nodes, depth & height*.

Proofs

Mathematical Statements:

- Definition, Lemma, Theorem, Corollary

Types of Proofs:

- Contradiction
- Induction
- Counter-example

Proof by Contradiction

Example: $\sqrt{2}$ is rational.

Proof by Induction

If we want to prove a statement $P(n)$ is true for all natural numbers $n \in \{1, 2, 3...\}$, we can achieve this with the following two steps:

1 Prove that the statement holds when $n = 1$
($P(1)$ is true). $- - - --$ **basis**

2 Prove that if the statement holds for $n = m$, then the same statement holds for $n = m + 1$.
$(P(m) \Rightarrow P(m + 1))$. $- - - --$ **induction step**

Example

$$\sum_{1}^{n} = \frac{n(n+1)}{2} \text{ for } n = \{1, 2, 3...\}.$$

Proof by Induction: Generalizations

Generalization type 1:

- If we want to prove a statement P not for all natural numbers but only for all numbers greater than a certain number b then the following two steps are sufficient

  1. **basis:** Prove that the statement holds when $n = b$.
  2. **induction step**: Prove that if the statement holds for $n = m$ then the same statement also holds for $n = m + 1$.

Generalizations

Generalization type 2:

- Another generalization allows that in the second step, we not only assume that the statement holds for $n = m$ but also for all n smaller than or equal to m. This leads to the following two steps.

  1. **basis:** Prove that the statement holds when $n = b$.
  2. **induction step**: Prove that if the statement holds for $n \leq m$ then the same statement also holds for $n = m + 1$.

Example

Every natural number greater than 1 is a product of prime numbers.