Discrete Mathematics Memorandum

1 Sets

- **Definition**: A **set** is an **unordered** collection of **distinct** objects. The objects in the set are called its **elements** or **members**.
- **Definition**: A is a **subset** of B ($A \subseteq B$) if every member of A is also a member of B. In the same circumstances we also say that B is a **superset** of A ($B \supseteq A$).
- **Definition**: A is a **proper subset** of B ($A \subset B$) if every member of A is also a member of B and some members of B are not member of A. In the same circumstances we also say that B is a **proper superset** of A ($B \supset A$).
- **Definition**: Two sets are **equal** ($A = B$) if the have exactly the same members.
- **Operations on sets**:
  1. **Union**: $A \cup B = \{x | x \in A \text{ or } x \in B\}$
  2. **Intersection**: $A \cap B = \{x | x \in A \text{ and } x \in B\}$
  3. **Relative complement**: $A \setminus B = \{x | x \in A \text{ and } x \notin B\}$
  4. **Symmetric difference**: $A \oplus B = x | (x \in A \text{ and } x \notin B) \text{ or } (x \notin A \text{ and } x \in B)$
  5. **Complement**: when there is a **universe** U, a set which contains all other sets we are interested in, we can also define $\overline{A} = U \setminus A$
  6. **Cartesian product**: $A \times B = \{(x, y) | x \in A \text{ and } y \in B\}$
  7. **Power set**: $P(A) = \{B | B \subseteq A\}$
- **Generalized operations**:
  1. **Union**: $\bigcup_{i=1}^{n} A_i = \{x | x \in A_i \text{ for some } i\}$
  2. **Intersection**: $\bigcap_{i=1}^{n} A_i = \{x | x \in A_i \text{ for all } i\}$
  3. **Product**: $\bigtimes_{i=1}^{n} = \{(x_1, x_2, \ldots, x_n) | x_i \in A_i \text{ for each } i\}$
- **Algebraic laws**:
  1. **Idempotence laws**:
  $$A \cup A = A \qquad A \cap A = A$$
  2. **Commutativity laws**:
  $$A \cup B = B \cup A \qquad A \cap B = B \cap A$$
  3. **Associativity laws**:
  $$(A \cup B) \cup C = A \cup (B \cup C) \qquad (A \cap B) \cap C = A \cap (B \cap C)$$
  4. **Distributivity laws**:
  $$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

5. **Zero and one laws**:
$$A \cup \emptyset = A \qquad A \cap \emptyset = \emptyset$$
6. **Cancellation laws**:
$$A \setminus A = \emptyset \qquad A \setminus \emptyset = A$$
7. **Involution law**:
$$A \setminus (A \setminus B) = A \cap B$$
8. **De Morgan's laws**:
$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C) \qquad A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$
9. **Right-distributivity laws**:
$$(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C) \qquad (A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$$
10. **Distributivity laws**:
$$A \times (B \cup C) = (A \times B) \cup (A \times C) \qquad A \times (B \cap C) = (A \times B) \cap (A \times C)$$

- **Definition**: The **size** of a set is called its **cardinality** ($|A|$ or $\#A$). For finite sets, this is just the number of elements in the set. For infinite sets, cardinality is more difficult to define.
- **Definition**: A **bag** is an **unordered** collection of objects (**not necessarily distinct**).

2 Functions

- **Definition**: An **interval** is a subset I of $\mathbb{R}$ with the **interval property**:
$$\text{If } x, z \in I \text{ and } x < y < z \text{ then } y \in I$$
- **Definition**:
  - Intervals which do not contain their endpoints are called **open** intervals.
  - Intervals which do contain their endpoints are called **closed** intervals.
  - Intervals which do contain one of their endpoints and do not containt the other are called **half-open** intervals.
- A **function** ($f : A \to B$). associates elements of one set with another. It consists of:
  - A set A called the **domain**,
  - A set B called the **codomain**,
  - A **map** which associates exactly one element of B to each element of A.

  Two functions are **equal** if **all 3 components** are the same.
- **Definition**: A **partial function** is a function that associates exactly **zero or one** elements of the codomain to each element of the domain.
- **Definition**: Let $f : A \to B$ be a function. We define the **image** of f to be
$$Im(f) = \{b \in B | f(a) = b \text{ for some } a \in A\}$$
- **Definition**: f is **onto** (or **surjective**) if
$$\forall b \in B, \exists a \in A \text{ such that } f(a) = b$$

- **Definition**: f is **1-1** (or **injective**) if

$$\forall a_1, a_2 \in A, a_1 \neq a_2, \text{ then } f(a_1) \neq f(a_2)$$

- **Definition**:f is **bijective** if it is both onto and 1-1.
- **Theorem**: If $f : A \to B$ is bijective, then $|A| = |B|$.
- **Definition**: If $f : A \to B$ and $f : B \to C$, then we define the **composition** of f and g to be

$$(g \circ f) : A \to C, \quad (g \circ f)(x) = g(f(x))$$

- **Definition**: If $f : A \to B$ and $g : B \to A$ satisfy both

$$g \circ f = id_A$$

$$f \circ g = id_B$$

, then g is the **inverse** of f and we write $g = f^{-1}$.

- **Theorem**: f has an inverse $\iff$ f is bijective
- **Definition**: If $f : A \to B$ and $A^{'} \subseteq A$, then we can define the **restriction** of f to $A^{'}$ to be

$$f|_{A'} : A^{'} \to B, \quad f|_{A'}(a) = f(a) \text{ for } a \in \ A^{'}$$

- **Definition**: A function $f : A \times A \to A$ is called a **binary operator** on A.
- **Definition**: A binary operator $\cdot$ on A:
  - is **idempotent** if $x \cdot x = x$, $\qquad \forall x \in A$
  - is **commutative** if $x \cdot y = y \cdot x$ $\qquad \forall x, y \in A$
  - is **associative** if $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\qquad \forall x, y, z \in A$
  - has an **identity element** e if $e \cdot x = x \cdot e = x$ $\qquad \forall x \in A$
- **Proof of the contrapositive**: Instead of proving $P \implies Q$, one can prove $\neg Q \implies \neg P$.
- **Proof by contradiction**: To prove P, assume $\neg P$ and reach a contradiction ($\perp$).

3 Counting

- **Law of sum**: Let P_1 and P_2 be properties of objects which are **exclusive**. The number of objects with **either** property is the number with property P_1 **plus** the number with property P_2.

$$A \cap B = \emptyset \implies |A \cup B| = |A| + |B|$$

- **Law of subtract**: Let P_1 and P_2 be properties, such that P_1 is true at least whenever P_2 is true. Then the number of objects with property P_1 **but not** P_2 is the number with property P_1 **minus** the number with property P_2.

$$B \subseteq A \implies |A \setminus B| = |A| - |B|$$

- **Law of product**: If counting the number of ways of making a sequence of choices and the choices are **independent**, then the total number of ways of making the sequence of choices is the **product** of the number of choices at each stage.

$$|A \times B| = |A| \cdot |B|$$

- Double counting: Instead of counting each element of a set once, one can count each of them m times, and then divide the result by m.

- **Definition**: The **factorial** of n is defined by

$$n! = 1 \cdot 2 \cdot \cdots \cdot n$$

- **Definition**: The **binomial coefficient** is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

- **Definition**: The **multinomial coefficient** is defined by

$$\binom{n}{n_1 n_2 \dots n_g} = \frac{n!}{n_1! n_2! \dots n_g!}$$

with $n_1 + n_2 + \cdots + n_g = n$

- **Theorem**:

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

- **Inclusion-Exclusion principle**:

$$|\bigcup_{i=1}^{n} A_i| = \sum_{k=0}^{n} (-1)^k \sum_{I \subseteq \{1,2,\dots,n\}, |I|=k} \bigcap_{i \in I} A_i$$

- **Definition**: The **floor function** rounds down real numbers to integers:

$$\lfloor - \rfloor : \mathbb{R} \in \mathbb{Z} \quad \lfloor x \rfloor = max\{n \in \mathbb{Z} | n \leq x\}$$

- **Definition**: The **ceil function** rounds up real numbers to integers:

$$\lceil - \rceil : \mathbb{R} \in \mathbb{Z} \quad \lceil x \rceil = min\{n \in \mathbb{Z} | n \geq x\}$$

4 Relations

- **Definition**: A relation on a set A is a subet of $A \times A$. More generally, a relation on sets A and B is a subset of $A \times B$.
- **Definition**: We say that a relation R is:
  - **reflexive** if aRa $\quad \forall a \in A$
  - **symmetric** if $aRb \implies bRa$ $\quad \forall a, b \in A$
  - **antisymmetric** if $aRb, bRa \implies a = b$ $\quad \forall a, b \in A$
  - **transitive** if $aRb, bRc \implies aRc$ $\quad \forall a, b, c \in A$
  - **irreflexive** if $a \not R a$ $\quad \forall a \in A$
  - **serial** if $\exists b \in A$ such that aRb $\quad \forall a \in A$
  - **total** if aRb or bRa $\quad \forall a, b \in A.$
- **Definition**: An **equivalence relation** on A is a relation which is reflexive, symmetric and transitive. If $\sim$ is an equivalence relation on A, then for each $a \in A$ we write

$$[a] = \{a^{'} \in A | a^{'} \sim a\}$$

. This is called the **equivalence class** of a.

- **Definition**: A **partition** of a set A is a collection of subsets $\{B_i | i \in I\} \subseteq P(A)$ satisfying

- $\bigcup_{i \in I} B_i = A$
- $B_i \cap B_j = \emptyset \quad \forall i \neq j$
- $B_i \neq \emptyset \quad \forall i$

- **Definition**: If R is a relation on A, we define the **converse** relation by

$$aR^{-1}b \quad \text{if} \quad bRa$$

.

- **Definition**: If R and S are both relations on A, we define their **composition** $S \circ R$ by

$$a(S \circ R)b \quad \text{if} \quad \exists x \in A \text{ sucht that } aRx \text{ and } xSb$$

- **Definition**: If R is a relation on A, we define the **transitive closure** of R by

$$aR^{+}b \quad \text{if} \quad \exists x_0, x_1, \dots, x_n \in A, n \geq 1 \text{ such that } a = x_0, x_0Rx_1, x_1Rx_2, \dots, x_{n-1}Rx_n, x_n = b$$

- **Definition**: If R is a relation on A, we define the **reflexive transitive closure** of R by

$$aR^{*}b \quad \text{if} \quad \exists x_0, x_1, \dots, x_n \in A, n \geq 0 \text{ such that } a = x_0, x_0Rx_1, x_1Rx_2, \dots, x_{n-1}Rx_n, x_n = b$$

- **Definition**: A **directed graph** consists of a set of **nodes** N and a set of **edges** $E \subseteq N \times N$. We say that there is an edge from n_1 to n_2 if $(n_1, n_2) \in E$.

5 Sequences

- **Definition**: A **sequence** is a function whose domain is $\mathbf{N}$ or $\mathbf{N}_{+}$: $(x_1, x_2, x_3, \dots)$
- **Definition**: A **recurrence relation** is a **recursive definition** of a sequence.
- **The principle of induction**: If $S(n)$ is a statement involving a natural number n, and we want to prove $S(n)$ for all n, we can:
  - prove $S(0)$
  - prove that, if $S(k)$, then $S(k+1)$.

  Then we may dedude that $S(n)$ is true, $\forall n \in \mathbb{N}$
- **The principle of strong induction**: If $S(n)$ is a statement involving a natural number n, and we want to prove $S(n)$ for all n, we can:
  - prove $S(0)$
  - prove that, if $S(j), \forall j \leq k$, then $S(k+1)$.

  Then we may dedude that $S(n)$ is true, $\forall n \in \mathbb{N}$
- **The minimal counterexample**: If we want to prove $S(n)$ for all natural numbers n, we suppose that it is not, and define m to be the smallest natural number for which $S(m)$ is false, and the prove that $S(m^{'})$ must also be false for some smaller natural number $m^{'}$.
- **Bell numbers**: The sequence (B_n), knows as the **Bell numbers**, has the following recurrence relation:

$$B_0 = 1, \quad B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_i$$

. Also,

$$B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$$

6 Modular arithmetic

- **Definition**: For a fixed positive integer n, we can define an equivalence relation $\equiv$ on $\mathbb{Z}$ by
$$x \equiv y \quad (mod\ n) \quad \text{if} \quad n|(x-y)$$
- **Method of repeated squaring**: An efficient way of computing x^y is:
$$x^y = \begin{cases} 1 & \text{if } y = 0 \\ x \cdot (x^2)^{\frac{y-1}{2}} & \text{if } y \text{ is odd} \\ (x^2)^{\frac{y}{2}} & \text{if } y > 0 \text{ is even} \end{cases}$$
.
- **Definition**: The **greatest common divisor** $gcd(m, n)$ is the largest integer dividing both m and n: $g = gcd(n, m)$ if
  - $g|m$
  - $g|n$
  - $l|m, l|n \implies l|g$
- **Euclid's algorithm**:

```
0. a := m; b := n;

1. q := a DIV b;
   r := a MOD b;

2. If r==0 return(b);
     else a := b;
          b := r;
          goto 1;
```

Computes $gcd(m, n)$.

- **Euclid's extended algorithm**:

```
0. a := m; b := n;    x := 0; y := 1; x' := 1; y' := 0;

1. q := a DIV b;          x := x' - (q * x);  x' := x;
   r := a MOD b;      y := y' - (q * y);  y' := y;

2. If r==0 return(b, x', y');
     else a := b;
          b := r;
          goto 1;
```

Computes $x, y \in \mathbb{Z}$ such that $gcd(m, n) = mx + ny$

- **Definition**: Fix a modulus n and let $x \in \mathbb{Z}$. A **multiplicative inverse** for x is an integer y satisfying
$$xy \equiv 1 \quad (mod\ n)$$
and we write $y \equiv x^{-1} \quad (mod\ n)$
- **Theorem**: If p is prime, every x with $x \not\equiv 0 \quad (mod\ p)$ has a multiplicative inverse $(mod\ p)$.
- **The pigeonhole principle**: You can't put more than n objects into n boxes without having at least two objects in the same box.

7 Asymptotic notation

- **Definition**: Suppose that f and g are both real-valued functions with domain $\mathbb{N}$. We write $f(n) = O(g(n))$ if there is a real number c and an integer N with
$$|f(n)| \leq c|g(n)|, \forall n \geq N$$
and say that f is **asymptotically bounded** by g.
- **Theorem**: $f(n) = O(g(n))$ is equivalent to existing a real number c such that
$$|f(n)| \leq c|g(n)|, \forall n \in \mathbb{N}$$
.
- **Definition**: We write $f(n) = \Omega(g(n))$ if $g(n) = O(f(n))$
We write $f(n) = \Theta(g(n))$ if $g(n) = O(f(n))$ and $f(n) = O(g(n))$

8 Orders

- **Definition**:
  - A **preorder** is a reflexive, transitive relation.
  - A **partial order** is a reflexive, antisymmetric, transitive relation.
  - A **linear order** (or **total order**)is an antisymmetric, transitive, total relation.
- **Definition**: For a set A, $a, b \in A$ and an order $\preceq$ on A, we say that a and b are **comparable** if $a \preceq b$ or $b \preceq a$.
- **Definition**: A **chain** is a subset of A of which all pairs are comparable.
- **Definition**: An **antichain** is a subset of A of which no pairs are comparable.
- **Definition**: For a set A and an order $\preceq$ on A, we can create the following orders on $A \times A$:
  - The **product order**: $(x, y) \preceq_P (x^{'}, y^{'}) \iff x \preceq x^{'}$ and $y \preceq y^{'}$
  - The **lexicographic order**: $(x, y) \preceq_L (x^{'}, y^{'}) \iff x \prec x^{'}$ or ($x \simeq x^{'}$ and $y \preceq y^{'}$)
- **Theorem**:
  - If $\preceq$ is a preorder/partial order/linear order on A, then $\preceq_L$ is a preorder/partial order/linear order on $A \times A$.
  - If $\preceq$ is a preorder/linear order on A, then $\preceq_P$ is a preorder/linear order on $A \times A$.
- **Definition**: A **Hasse diagram** is a graph, drawn in the plane, with vertices corresponding to the elements of A and an edge going from a to b if $a \prec b$ and there is no element x with $a \prec x \prec b$. This construction, which removes reflexive loops and all edges which follow by transitivity, is knows as the **cover relation**.
- **Definition**: Let A be a set ordered by a partial order $\preceq$ and let $S \subseteq A$.
  - An element $m \in A$ is an **upper bound** for S if $x \preceq m, \forall x \in S$.
  - An element $m \in A$ is a **lower bound** for S if $m \preceq x, \forall x \in S$.
  - m is the **maximum** of S if it is an upper bound and $m \in S$.
  - m is the **minimum** of S if it is a lower bound and $m \in S$.
  - m is a **least upper bound** (lub) for S if
    - m is an upper bound for S
    - if $m^{'}$ is any other upper bound for S, then $m \preceq m^{'}$.
  - m is a **greatest lower bound** (glb) for S if
    - m is a lower bound for S
    - if $m^{'}$ is any other lower bound for S, then $m^{'} \preceq m$.
- **Definition**: If every pair of a set has a lub and glb, the the order is called a **lattice**.
  If every subset has a lub and glb, then the order is called a **complet lattice**.
- **Definition**: Let A and B be sets, with orders $\preceq_A$ and $\preceq_B$. An **order isomorphism** between A and B is a bijection $f : A \to B$ satisfying
  $$a \preceq_A a^{'} \iff f(a) \preceq_B f(a^{'})$$
  .
- **Theorem**: If $\preceq$ is a linear order on A, these are equivalent definitions to lub/glb:
  - m is a **least upper bound** (lub) for S if
    - m is an upper bound for S

        - if $a \prec m$ then there is an element $x \in S$ with $a \prec x$
    - m is a **greatest lower bound** (glb) for S if
        - m is a lower bound for S
        - if $m \prec a$ then there is an element $x \in S$ with $x \prec a$

- **Theorem**: If there is an order isomorphism between A with $\preceq_A$ and B with $\preceq_B$, then, if $\preceq_A$ is a partial order/linear order/lattice, then so is $\preceq_B$ (and vice versa).