Week 7: Set Theory

Agenda:

- Basic Definitions and Properties of Sets
- Boolean Algebra, Russell's Paradox and the Halting Problem

Reading:

- Textbook: Chapter 5

- **Set:** A term that is used as **undefined**, basic in Set Theory
- Some important "properties":
  - A **well-defined** collection of objects:

    For any object, we are able to determine whether or not it is in the set.
  - Such an object is called an **element** of the set
  - Notation: $a \in A$, $a \notin A$
- A set can be designated by listing its elements, or describing the properties of its elements in a **universe**

  e.g., $A = \{1, 2, 3, 4, 5\} = \{x \mid x \in \mathcal{U}, 1 \leq x \leq 5\}$, where $\mathcal{U}$ denotes the set of integers
- The order is **irrelevant**
- **Subset**: $C \subseteq D$ iff every element of C is an element of D

  Or says, C is contained in D, D contains C
- $C \nsubseteq D \Leftrightarrow \exists x$ such that $x \in C$ and $x \notin D$
- **Proper** subset: $C \subset D$ iff $C \subseteq D$ and $\exists x$ such that $x \in D$ and $x \notin C$
- **Equal**: $C = D$ iff $C \subseteq D$ and $D \subseteq C$
- Null/empty set $\emptyset$ or $\{\ \}$
- **Size/cardinality** of a set A is $|A|$, which is the number of elements in A

Set Operations (given a universe $\mathcal{U}$):

- The **union** of A and B:

  $A \cup B = \{x \mid x \in A \vee x \in B\}$

- The **intersection** of A and B:

  $A \cap B = \{x \mid x \in A \wedge x \in B\}$

- The **difference** of B minus A (or **relative complement** of A in B):

  $B - A = \{x \mid x \in B \wedge x \notin A\}$

- The **complement** of A:

  $A^c = \mathcal{U} - A = \{x \mid x \notin A\}$

- The **symmetric difference** of A and B:

  $A \triangle B = (A - B) \cup (B - A)$

- A and B are **disjoint** iff $A \cap B = \emptyset$

- A_1, A_2, ..., A_n are **mutually disjoint** iff $A_i \cap A_j = \emptyset$ for all i, j, $i \neq j$

  e.g. if $A_1 = \{x \in Z | x = 3k$ for some $k\}$, $A_2 = \{x \in Z | x = 3k + 1$ for some $k\}$ and $A_3 = \{5\}$ then A_1, A_2, A_3 are mutually disjoint.

- **Partition** of a set A: a collection of subsets $A_1, A_2, \ldots, A_n$ of A

  - $A = A_1 \cup A_2 \cup \ldots \cup A_n$
  - $A_1, A_2, \ldots, A_n$ are mutually disjoint

  e.g. if $A_1 = \{x \in Z | x = 3k$ for some $k\}$, $A_2 = \{x \in Z | x = 3k + 1$ for some $k\}$ and $A_3 = \{x \in Z | x = 3k + 2$ for some $k\}$ then A_1, A_2, A_3 partitions Z.

- **Power set** of a set A, denoted as $\mathcal{P}(A)$, is the collection of all subsets of A.

  e.g. if $A = \{1, 2, 3\}$ then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

- **Theorem:** For every $n \geq 0$, the size of the power set of every set of size n is 2^n.

Proof: Let $S(n)$ be the predicate: "the size of the power set of every set of size n is 2^n".

We prove $S(n)$ for all $n \geq 0$ by induction on n.

Basis: for $n = 0$ we have the empty set and clearly it has only one subset. So $S(0)$ holds.

Ind. Step: Let $k \geq 0$ be an arbitrary integer and assume that $S(k)$ holds. We prove $S(k+1)$.

Let $A = \{e_1, \ldots, e_{k+1}\}$ be an arbitrary set of size $k+1$. We partition the subsets of A into two groups G_1 and G_2: G_1 consist of those subsets of A that do NOT include e_{k+1} and G_2 consist of those subsets of A that include e_{k+1}.

Clearly every subset of A belongs to exactly one of G_1 or G_2. Since every subset of A in G_1 is a subset of $A' = \{e_1, \ldots, e_k\}$ too, by ind. hyp. $|G_1| = 2^{|A'|} = 2^k$.

Also, every subset of A in G_2 is obtained by adding e_{k+1} to a subset of A that is in G_1 (similarly, every subset of A in G_1 is obtained by removing e_{k+1} from the corresponding subset of A in G_2). Thus $|G_2| = |G_1| = 2^k$.

Thus $|\mathcal{P}(A)| = |G_1| + |G_2| = 2.2^k = 2^{k+1}$, as wanted.

- (Ordered) n-**tuple**: $(x_1, x_2, \ldots, x_n)$
  - $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n)$ iff $x_i = y_i$ for all i

  e.g. $(1, 2) \neq (2, 1)$.

- The **Cartesian product** of $A_1, A_2, \ldots, A_n$ is

  $A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i = 1, 2, \ldots, n\}$

The Laws of Set Theory:

- Some subset relationships:
  - $A \cap B \subseteq A$
  - $A \subseteq A \cup B$

  - If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$
  - E.g., prove that $A \subseteq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A \Leftrightarrow B^c \subseteq A^c$

- Proof of the above relationships, in general
  - how to prove that $A \subseteq B$ (subset relation)?
  - how to prove that $A = B$ (set identity)?

- Example: Prove that for all sets A, B, $A \cap B \subseteq B$.

  Proof: Let A and B any pair of sets and let x be an arbitrary element of $A \cap B$.

  From definition of $A \cap B$, $x \in A \wedge x \in B$. Thus $x \in B$.

- Similarly can be shown: $A \cap B \subseteq A$ and $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

- Example: Prove that $A \subseteq B \leftrightarrow A \cup B = B$

  We prove $A \subseteq B \rightarrow A \cup B = B$. The other direction is similar.

  To prove $A \cup B = B$ we need to show: i)$B \subseteq A \cup B$ and ii) $A \cup B \subseteq B$

  Part (i) is easily done in the manner in previous example.

  For part (ii) we assume $A \subseteq B$ and show $A \cup B \subseteq B$.

  Let x be an arbitrary element from $A \cup B$. Then $x \in A \vee x \in B$.

  Case 1: if $x \in B$ then we are done.

  Case 2: if $x \in A$, then because $A \subseteq B$, $x \in B$ too.

  In both cases, $x \in B$, and therefore $A \cup B \subseteq B$, as wanted.

- **Theorem:** For all subsets A, B, C of a universe U we have:
  1. $A \cup B = B \cup A$, $A \cap B = B \cap A$,
  2. $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$,
  3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
  4. $A \cup \emptyset = A$, $A \cap U = A$

5. $A \cup A^c = U$, $A \cap A^c = \emptyset$,
6. $(A^c)^c = A$
7. $(A \cup B)^c = A^c \cap B^c$, $(A \cap B)^c = A^c \cup B^c$
8. $A - B = A \cap B^c$
9. $U^c = \emptyset$, $\emptyset^c = U$

- Example: Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

  We need to show that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

  We prove the first one. The proof of the other direction is similar.

  Let x be an arbitrary element of $A \cup (B \cap C)$. Thus $(x \in A) \vee (x \in B \cap C)$.

  From the definition of intersection: $(x \in A) \vee [(x \in B) \wedge (x \in C)]$. Thus $[(x \in A) \vee (x \in B)] \wedge [(x \in A) \vee (x \in C)]$.

  This implies $(x \in A \cup B) \wedge (x \in A \cup C)$; and therefore $x \in (A \cup B) \cap (A \cup C)$.

Boolean Algebra:

- A set B together with two operations ($+$ and $\cdot$), such that for all $a, b \in B$, $a + b, a \cdot b \in B$ (**closed**), and

  1. **Commutative Laws**: $a + b = b + a$ and $a \cdot b = b \cdot a$
  2. **Associative Laws**: $(a+b)+c = a+(b+c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  3. **Distributive Laws**: $a + (b \cdot c) = (a + b) \cdot (a + c)$ and $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
  4. **Identity Laws**: there exist distinct elements 0 and 1 in B, such that

     $a + 0 = a$ and $a \cdot 1 = a$
  5. **Complement Laws**: for each $a \in B$, there exists an element $\overline{a} \in B$ such that

$a + \overline{a} = 1$ and $a \cdot \overline{a} = 0$

- $\mathcal{P}(\mathcal{U})$ together with $\cup$ and $\cap$ is a Boolean algebra

  $\cup$ corresponds to $+$ and $\cap$ corresponds to .,

  $0 = \emptyset$ and $1 = \mathcal{U}$,

Russell's Paradox:

- Define $S = \{A \mid A$ is a set and $A \notin A\}$

  Is S a set? or, is S an element of itself?

- It is not possible to prove, in a **mathematically** rigorous way, that **mathematics** is free of contradiction.

- The **Halting Problem**: Is there an algorithm that will accept any algorithm A and any dataset D as input and will then print "halts" or "loops forever" to indicate whether A terminates in a finite number of steps or loops forever when run on dataset D?

  No.

  Proof by contradiction (as in the tex).