< Summary of Set Theory and Induction >

Discussed in class:

- Informally, a set is a collection of objects (at a conceptual level) that share some common property.
- We can define a set by either list out the members of the set explicitly (this is fine if the set is finite and small) or write out the conditions which the members of a set must all satisfy (this is better if the set is large but its members have some common properties).
- Not all objects can desirably be a set, as illustrated by Russell's Paradox.

Definition Let A and B be two sets.

A is a subset of B (denoted by $A \subseteq B$) if every element of A is also an element of B.

A is a proper subset of B (denoted by $A \subset B$) if $A \subseteq B$ and there exists at least one element in B that is not in A.

A and B are equivalent (denoted by $A = B$) if both $A \subseteq B$ and $B \subseteq A$.

Definition An empty set $\emptyset$ is a set which contains no member.[I]

Definition The cardinality of a set A, denoted by $|A|$, is the number of elements in A.

Definition The power set of a set A, denoted as $P(A)$, is the set of all subsets of A.

Theorem If A is a finite set, then $|P(A)| = 2^{|A|}$.

Theorem $A \subseteq B$ iff $P(A) \subseteq P(B)$.

Definition Let A and B be two subsets of some set U.

The union of A and B is the set

$$A \cup B = \{x \in U | x \in A \; or \; x \in B\}$$

The intersection of A and B is the set

$$A \cap B = \{x \in U | x \in A \; and \; x \in B\}$$

The setwise difference[II] of A subtract B is the set

$$A - B = \{a \in A | a \notin B\}$$

Definition Let U be a set and let A be a subset of U. The complement of A, denoted by A^c, is the set

$$A^c = \{x \in U | \; x \notin A\}$$

Corollary $A^c = U - A$

Theorem (De Morgan's Law)

For sets $A, B \subseteq U$,

$$(A \cup B)^c = A^c \cap B^c \quad \text{and} \quad (A \cap B)^c = A^c \cup B^c$$

[I] The empty set is a subset of every set and is unique. These two facts can be proven quickly by exploiting the conditional statement of first-order logic.

[II] *$A - B$ is sometimes denoted by $A \backslash B$.

Definition The Cartesian Product of two sets A and B is the set of ordered pairs[III]

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

Definition A relation between A and B is a subset of $A \times B$.

Definition A function from a set A to a set B, denoted as $f: A \longrightarrow B$, is a subset of $A \times B$ which satisfies the following two properties:

1. For all $a \in A$, there exists some $b \in B$ such that $(a,b) \in f$.
2. For all $a \in A$, if $(a,b) \in f$ and $(a,c) \in f$, then $b = c$.[IV]

Definition Let A and B be two sets such that $A \subseteq B$.

The characteristic function of A in B is the function $\chi_A: B \longrightarrow \{0,1\}$ of the form

$$\chi_A(b) = \begin{cases} 0 & if\ b \in A \\ 1 & if\ b \notin A \end{cases}$$

Definition A function $f: A \longrightarrow B$ is injective (or one-to-one) if, for all $a_1, a_2 \in A$, $f(a_1) = f(a_2)$ implies $a_1 = a_2$.

Definition A function $f: A \longrightarrow B$ is surjective (or onto) if, for all $b \in B$, there exists some $a \in A$ such that $f(a) = b$.[V]

Definition A function $f: A \longrightarrow B$ is bijective if it is both injective and surjective.

Theorem If $f: A \longrightarrow B$ and $g: B \longrightarrow C$ are injective, then $g \circ f: A \longrightarrow C$ is injective. (A similar result holds for surjectivity and bijectivity.)

Definition Let $f: A \longrightarrow B$, then the inverse function of f, denoted as $f^{-1}: B \longrightarrow A$, is a function such that $f^{-1}\big(f(a)\big) = a$ for all $a \in A$ and $f\big(f^{-1}(b)\big) = b$ for all $b \in B$.

Theorem Let $g: A \longrightarrow B$. g is bijective if and only if g^{-1} exists.

Definition Two sets A and B are equinumerous, denoted by $|A| = |B|$, if there exists some bijection $f: A \longrightarrow B$.

Theorem Suppose that A and B are finite sets with $|A| = m$ and $|B| = n$. If there is a bijection $f: A \longrightarrow B$, then $m = n$.

Theorem For any sets A, B and C,

1. $|A| = |A|$
2. $|A| = |B|$ if and only if $|B| = |A|$
3. If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.[VI]

[III] An ordered pair (a,b) is defined as the set $(a,b) = \{\{a\}, \{a,b\}\}$. This definition gives the properties that coincide with what we mean intuitively by an ordered pair, namely that $(a,b) = (c,d)$ iff $a = b$ and $c = d$ (ie. the idea of coordinate correspondence and that the order of arrangement matters).

[IV] The set A is the domain of f; the set B is the codomain of f; the range of f is the subset $rng(f) \subseteq B$ such that, for all $b \in rng(f)$, there exists some $a \in A$ such that $(a,b) \in f$.

[V] This means that the range of the function must be equal to its codomain.

[VI] These show that being equinumerous is an equivalence relation.

Theorem For two sets A and B,

1. $|A| \leq |B|$ iff there is an injection $f: A \longrightarrow B$.
2. $|B| \leq |A|$ iff there is a surjection $g: A \longrightarrow B$.

Definition A set S is denumerable (or infinitely countable) if $|S| = |\mathbb{N}|$. S is countable if it is finite or denumerable, otherwise S is said to be uncountable.[VII]

Lemma If S is a set whose members can be listed as

$$S = \{s_1, s_2, s_3, \dots\}$$

where $s_i \neq s_j$ for all $i, j \in \mathbb{N}$, then $|S| = |\mathbb{N}|$.

Theorem The set of all real numbers is uncountable.

Definition The Pascal's Triangle is an arrangement of natural numbers which has the two following properties:

Let $b_{i,j}$ be the entry at the i-th row and j-th column, then, for all $i, j \in \mathbb{N}_0$,

1. $b_{i,0} = b_{i,i} = 1$
2. $b_{i,j} = b_{i-1,j} + b_{i-1,j-1}$

Definition $\binom{i}{j}$ is the number of ways of choosing j objects from a collection of i objects.

Theorem For all $i, j \in \mathbb{N}_0$,

$$\binom{i}{j} = \binom{i-1}{j} + \binom{i-1}{j-1}.$$

Theorem For all $i, j \in \mathbb{N}_0$,

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

Definition A set S is well-ordered if every subset $S' \subseteq S$ has a least element.

Axiom $\mathbb{N}$ is well-ordered.

Theorem (The Principle of Mathematical Induction, General Form)

Let $P(n)$ be a statement whose truth value depends on $n \in \mathbb{N}$.

If, for some $m \in \mathbb{N}$

1. $P(m)$ is true
2. For an arbitrary $n \in \mathbb{N}$ such that $n \geq m$, $P(n)$ is true implies $P(n+1)$ is true

then $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq m$.

Theorem (The Strong Principle of Mathematical Induction, General Form)

[VII] We denote the cardinality of a denumerable set by $\aleph_0$ (aleph-naught).

Let $P(n)$ be a statement whose truth value depends on $n \in \mathbb{N}$.

If, for some $m \in \mathbb{N}$

1. $P(m)$ is true
2. For an arbitrary $n \in \mathbb{N}$, $P(k)$ is true for all $m \leq k \leq n$ implies $P(n+1)$ is true

then $P(n)$ is true for all $n \in \mathbb{N}$ such that $n \geq m$.

Definition The Fibonacci Numbers are a sequence of integers defined recursively as follows:

$F_1 = 1$

$F_2 = 1$

$F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$

Theorem For all $n \in \mathbb{N}$, F_n and F_{n+1} are relatively prime.

Discussed in the textbook:

p. 25 A collection S of nonempty subsets of some set A s a partition of A such that

1. For all $X,Y \in S$, either $X = Y$ or $X \cap Y = \emptyset$. ("mutual exclusiveness")
2. $\bigcup_{X \in S} X = A$ ("exhaustiveness")[VIII]

p. 144 (Proof by Minimum Counterexample)

To show that $P(n)$ is true for all $n \in \mathbb{N}$, we can also use proof by contradiction as follows:

1. Assume that there exists some $n \in \mathbb{N}$ such that $P(n)$ is false.
2. By the Well-Ordered Principle, there exists some smallest integer m such that $P(m)$ is false. (m is the minimum counterexample)
3. Since m is the minimum counterexample, $P(k)$ is true for all $1 \leq k < m$.
4. Derive a contradiction. (This is usually achieved by contradicting the idea that $P(m)$ is false.)

p. 212 A bijective function $f: A \longrightarrow A$ is also called a permutation.

Theorem 10.3 Every infinite subset of a denumerable set is denumerable.

Result 10.5 If A and B are denumerable, then $A \times B$ is denumerable.

p. 237 Let $f: A \longrightarrow B$ and let D be a nonempty subset of A. The restriction f_1 of f to D is the function

$$f_1 = \{(a,b) \in f \mid a \in D\}$$

Theorem 10.17 Let A and B be nonempty sets such that $B \subseteq A$. If there exists an injective function from A to B, then there exists a bjective function from A to B.

Theorem 10.18 (The Schröder-Bernstein Theorem)

If $\boldsymbol{A}$ and $\boldsymbol{B}$ are sets such that $|\boldsymbol{A}| \leq |\boldsymbol{B}|$ and $|\boldsymbol{B}| \leq |\boldsymbol{A}|$, then $|\boldsymbol{A}| = |\boldsymbol{B}|$.

[VIII] One can generate an equivalence class from a partition, and similarly generate a partition from an equivalence class.

Axiom (p.240) (The Axiom of Choice)
For every collection of pairwise disjoint nonempty sets, there exists at least one set that contains exactly one element of each of these nonempty sets.

Theorem 10.19 The sets $P(\mathbb{N})$ and $\mathbb{R}$ are equinumerous.

Important Topics:

- Know how to prove set relations
- Know how to prove properties of functions as well as constructing injections, subjections or bijections between two sets
- Know how to work with cardinalities of sets
- Cantor's Diagonalization argument
- Prove the Fundamental Theorem of Arithmetic by using strong induction
- Being able to spot patterns and form a conjecture for your inductive proof
- Perform induction on summation identities, divisibility, inequalities and set identities
- Performing strong induction on recursively-defined sequences
- Know how to prove the Schröder-Bernstein Theorem

Some well-known summation identities:

$$\sum_{j=0}^{i} \binom{i}{j} = 2^i \qquad \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \qquad \sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2$$