Naive Set Theory

Yashas.N

1 Axioms of Set Theory

1. **Axiom of Extension** : Two sets are equal if only if they have the same elements.

2. **Axiom of Specification** : To every set A and to every condition $S(x)$ there corresponds a set B whose elements are exactly those elements x of A for which $S(x)$ holds i.e.

$$\exists\, B = \{x \in A : S(x)\}$$

where $S(x)$ is being stated as to hold true.

3. **Axiom of Pairing** : For any two sets there exists a set that they both belong to i.e. for sets A and B

$$\exists\, C : A \in C \text{ and } B \in C$$

4. **Axiom of Union** : For every collection of sets there exists a set that contains all elements that belong to at least one set of the given collection i.e. for a set collection $\mathscr{C}$

$$\exists\, U = \{x : x \in X \text{ for some } X \in \mathscr{C}\} = \bigcup_{X \in \mathscr{C}} X$$

5. **Axiom of Powers** : For each set there exists a collection of sets that contains among its elements all the subsets of the given set i.e. for given set

$$\exists P(A) = \{X : X \subset A\}$$

6. **Axiom of Infinity** : There exist a set containing 0 and containing the successor of each element. (here it is customary to define $0 = \phi$= empty set , successor of $x = x^+ = x \cup \{x\}$).

7. **Axiom of Choice** : The Cartesian product of non empty family of non empty sets is non empty.
Can be interpreted as : There exist a function (f) whose domain is collection of non empty sets ($\{A_i\}$) (can be infinitely many) such that $f(A_i) \in A_i$ for each i (here the function chooses an element of the set so is called a choice function hence name of the theorem).

8. **Axiom of substitution** : If $S(a, b)$ is a sentence such that for each a in a set A the set $\{b : S(a, b)\}$ can be formed, then there exists a function F with domain A such that $F(a) = \{b : S(a, b)\}$ for each a in A. (i.e. this axiom enables to make new sets out of old sets by substituting for old elements in the new elements, i.e. informally any manipulations one can do to the elements of a set yields a set).

2 Set properties and generalizations

2.1 Standard Definitions

• Complement of set A (A') : $A' = \{x : x \notin A\}$, here x is taken from set E, where a set E is assumed to contain all other sets involved in the particular needed operations.

• Subset : B is subset of A ($B \subset A$) iff $x \in B \implies x \in A$
• Proper subset : $A \subsetneq B$ iff $A \subset B$ and $A \neq B$
• Union : $A \cup B = \{x : x \in A \text{ or } x \in B\}$,
• Intersection : $A \cap B = \{x : x \in A \text{ and } x \in B\}$
• Symmetric Difference : $A \ominus B = (A \cup B) - (A \cap B)$ (gives elements only in A or B but not in both).

2.2 Laws concerning sets

• **De Morgan laws** :

$$(A \cup B)' = A' \cap B'$$
$$(A \cap B)' = A' \cup B'$$

• **Principle of Duality** of sets : If in an inclusion or equation involving unions, intersections, and complements of subsets of E we replace each set by its complement, interchange unions and intersections, and reverse all inclusions, the result is another theorem (i.e. holds true).
• Some properties :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$A - B = A \cap B'$$
$$A - (A - B) = A \cap B$$
$$A \cap (B - C) = (A \cap B) - (A \cap C)$$
$$A \cap B \subset (A \cap C) \cup (B \cap C')$$
$$(A \cup C) \cap (B \cup C') \subset A \cup B$$
$$P(A \cap B) = P(A) \cap P(B)$$
$$P(A) \cup P(B) \subset P(A \cup B)$$

3 Generalizations

3.1 Relations

• An ordered pair (a, b) can be denoted by $\{\{a\}, \{a, b\}\}$
• A relation from set X to set Y (xRy) is a subset of all ordered pairs from X and Y in the form $R \subset \{(x, y) : a \in X \text{ and } b \in Y\}$
• set X is called Domain of R ($Dom(R)$) and set Y is called range of R ($Ran(R)$).
• a Relation from X to X is called an Equivalence Relation iff (if and only if) it is Reflexive (xRx or $(x, x) \in R \ \forall x \in X$), Symmetric ($xRy \implies yRx$ or $(x, y) \in R \implies (y, x) \in R$) and Transitive ($xRy, yRz \implies xRz$ or $(x, y), (y, z) \in R \implies (x, z) \in R$).

3.2 Functions

• A function from $f : X \to Y$ is a relation $f : X$ to Y such that $Dom(f) = X$ and for each $x \in X$ there exists a unique $y \in Y$ such that $f(x) = y$ (i.e. xfy_1 , xfy_2 then $y_1 = y_2$).
• A function $x : I \to X$ is sometimes called a family , I is an index set, X is indexed set, $i \in I$ is called index and $x_i = x(i)$ and $Ran(I)$ is often called as a family $\{x_i\}$ in X (here in general I is some standard set like $\mathbb{N}, (a, b)$).
• $\bigcup_{i \in I} A_i$ (say for $A : I \in P(X)$) means union of range of function A (subsets of X) with domain in I. This is often called arbitrary union.
• Similarly $\bigcap_{i \in I} A_i$ is arbitrary intersection.
• Laws or properties regarding unions and intersections hold for arbitrary indexes.

• **preimage of a function** f^{-1} : for function $f : A \to B$ define function $f^{-1} : P(B) \to P(A)$ such that for every $Y \subset B$, $f^{-1}(Y) = \{x \in A : f(x) \in Y\}$
• a function is one-one iff every distinct element in the domain is mapped to distinct element in the range i.e. f is $1-1$ function iff $f(x_1) = f(x_2) \iff x_1 = x_2$.
• a function $f : A \to B$ is onto iff $Ran(f) = B$
• $f(f^{-1}(Y)) \subset Y$ and $f(f^{-1}(Y)) = Y$ iff f is onto
• $X = f^{-1}(f(X))$ and $f^{-1}(f(\{x\})) = \{x\}$ iff f is one-one
• for any function $f : A \to B$ and if $f(A_i) = \{f(a) | a \in A_i\}$ then

$$f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i).$$

$$f(\bigcap_{i\in I} A_i) \subset \bigcap_{i\in I} f(A_i).$$

$$f^{-1}(\bigcup_{i\in I} B_i) = \bigcup_{i\in I} f^{-1}(B_i).$$

$$f^{-1}(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^{-1}(B_i).$$

for every $\bigcup_{i\in I} A_i \subset A$:

$$f(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} f(A_i) \iff f \text{ is one-one.}$$

- $f^{-1}(B - Y) = A - f^{-1}(Y)$ (for $f : A \to B$)
(i.e. $f^{-1}(Y^c) = (f^{-1}(Y))^c$ where ^{c} denotes respective complements)
- for all $X \subset A$:
$f(A - X) \subset B - f(X)$ iff f is one-one.
$B - f(X) \subset f(A - X)$ iff f is onto.
$\implies f(A - X) = B - f(X)$ iff f is bijective.
- if A and B are finite sets such that $|A| = n$ and $|B| = m$ then
  - Number of functions from $A \to B$ is equal to m^n
(use : each element of A has $|B|$ choices to be mapped to)
  - Number of one-one functions from $A \to B$ is equal to $\binom{m}{n} n! = \frac{m!}{(m-n)!}$
(is possible iff $|B| \geq |A|$, use: first choose n elements from B and each of these can form $n!$ ordered pairs)
  - Number of onto functions from $A \to B$ is equal to $\sum_{i=0}^{m-1} (-1)^i \binom{m}{i} (m-i)^n$
(is possible iff $|A| \geq |B|$)

3.3 Cartesian Product

- Cartesian product between family of sets $\{X_i\}$ with index set I can be defined as a set of all families $\{x_i\}$ such that $x_i \in X_i$ with each $i \in I$ (i.e. $(a_1, a_2, ...) = \{x_i\} = \{x(1), x(2), ...\}$ for some family x with index set I satisfying condition $x_i \in X_i$)
- Usually Cartesian product of two sets can be defined as an ordered pair itself.

3.4 Order

- A relation R in X is called a **partial order** if R is reflexive, anti-symmetric (i.e. $xRy, yRx \implies x = y$) and transitive
- a partial order is **total order** iff
$\forall x, y \in X$ xRy or yRx holds.
- a totally ordered set is called a chain.
- We can construct Natural numbers by Axiom of infinity : defining successor set (S) as set containing $o = \phi$ and if $n \in S$ then $n^+ = n \cup \{n\} \in S$ and ($\omega = \mathbb{N} \cup \{o\}$) as the intersection of all successor sets.
- **Peano's Axioms** (properties of ω):
  1. $o \in \omega$,
  2. $n \in \omega \implies n^+ \in \omega$,
  3. **Principle of mathematical Induction** : if $S \subset \omega$, $o \in S$ and if $n^+ \in S$ whenever $n \in S$ then $S = \omega$,
  4. $n^+ \neq o \; \forall n \in \omega$
  5. $n, m \in \omega$ and if $n^+ = m^+$ then $n = m$
- A **sequence** is a function from ω to X(any set).
- **Recursion Theorem** : if a is an element of set X and if function $f : X \to X$ then there exists a function $u : \omega \to X$ such that $u(o) = a$ and $u(n^+) = f(u(n))$ (i.e. there exists recursive sequences which can be defined from a single elements of a set and a function on the set).
- if X is a partially ordered set then it can be converted to a totally ordered one by replacing the corresponding relation.
- if $\leqq$ is partial ordering of X then:
  - $\forall x \in X$ if $x \leqq a$ then a is an upper bound if $a \in X$ and $a \leqq x \implies a = x$ then a is maximal element.
- **Zorn's Lemma** : if X is a partially ordered set such that every chain in X has an upper bound then X contains a maximal element.
- a partially ordered set X has a least element say a if $x \leqq a$ for $x \in X$ then $a = x$.

• a partially ordered set X is well ordered iff every subset of X has a least element

• Every well ordered set is a totally ordered.

• **Well ordering Theorem** : Every set can be well ordered
(note: not every partial order can be made well ordering but the underlying set (domain) can be well ordered by 'a' order).

• **Principle of Transfinite Induction** : If X is well ordered set and $S \subset X$ such that if all elements $s \leqq x$ belong to S then $x \in S$ then $S = X$

• Axiom of Choice $\iff$ Zorn's Lemma $\iff$ Well ordering theorem

• for a well ordered set W and any set X :

▪ for $a \in W$, A sequence of type a in X is a function from initial segment of a ($s(a) = \{b \in w : b < a\}$ for well ordering $<$) into X

▪ eg : if U is a function from W to X then U^a which is restriction of U till $s(a)$ is a sequence of type a in X.

▪ A sequence function of type W in X is a function whose domain is sets of sequences of type a in X for all a in W and range is in X. (this is sort of extension of sequences of type a in X by adding $f(s(a))$ to it to elongate it).

• **Transfinite Recursion Theorem** : if W is a well ordered set and f is sequence function of type W in X then there exists a unique function $U : W \to X$ such that $U(a) = f(U^a)$.
i.e. a recursive function exists such that its value at a depends only on $s(a)$ and their function values.

• Two partially ordered sets are similar if there exists an order preserving one to one correspondence and onto function between them i.e. $X \simeq Y \iff \exists f : X \to Y : a \leqq b \implies f(a) \leqq f(b)$, f is called the similarity.

• if f is similarity from X to Y clearly f^{-1} is also a similarity from Y to X.

• **if f is a similarity of well ordered set X onto itself then $a \leqq f(a)$ $a \in X$**

• Consequence of preceding point :

▪ if two well ordered sets are similar the their similarity is unique

▪ any well ordered set X is not similar to any $s(a)$ $(a \in X)$ i.e. well ordered set is not similar to initial segment of any of its element.

▪ Two well ordered sets are similar or one of them is similar to an initial segment of the other.

4 Numbers

• As we have defined $\omega = \mathbb{N} \cup \{o\}$ some of the properties of it are as follows (may not be related to 'real world' $\mathbb{N}$ at all):

▪ if $n < m$ then $n \in m$
(recall that we defined $n^+ = n \cup \{n\}$)

▪ from above point n contains all its predecessors ($\{m : m < n\}$)

▪ initial segment of $n = s(n) = n$
(remark : here 'n' from definition is a set of set of sets ... of set containing ϕ, weird but holds logically).

▪ if $n \neq o$ then $n = m^+$ for some $m \in \omega$

4.1 Arithmetic in ω

• Addition : from recursion theorem we can find a function $s_m : \omega \to \omega$ such that $s_m(o) = m$ and $s_m(n^+) = (s_m(n))^+$ thus $m + n$ is just $s_m(n)$.

• other arithmetic operations and their usual properties can be obtained from the already defined addition operation and recursion theorem.

4.2 Equivalence

• Two set E and F are equivalent ($E \sim F$) if there exists a one-one correspondence between them (i.e. $f : E \to F$ such that f is bijective).

• every proper subset of ω is equivalent to one of the elements of ω

• a set is finite if it is equivalent to an element in ω otherwise it is infinite

• ω is infinite

5 Ordinal Numbers

• From Axiom of substitution we can extend the set ω to count beyond infinite sets like $\{\omega, \omega^+, (\omega^+)^+, ..\}$ can be formed

• Ordinal numbers are well ordered set α such that initial segment of a: $s(a) = a$, $\forall a \in \alpha$

• clearly $n \in \omega$, ω, ω^+,... are all ordinal numbers

• let $\omega + n$ denote the nth successor of ω (eg : $\omega + 2 = (\omega^+)^+ = \omega^+ \cup \{\omega^+\} = \{\omega, \{\omega\}, \{\omega, \{\omega\}\}\}$)

• the set $\{\omega, \omega^+, (\omega^+)^+, ..\}$ is nothing but $((\omega^+)^+)^{\cdot\cdot} = \omega + \omega$ infinite times denote this set by $\omega 2$

• $\omega 2 + n = ((\omega 2^+)^+)^{\cdots}$ n times

• let $\omega 2 + \omega = \omega 3$ and $\omega 3 + \omega = \omega 4$ and so on til we reach ω then denote $\omega\omega$ as ω^2 and continuing this process we get $\omega^2\omega = \omega^3$ similarly we get ω^ω which is denoted by ϵ_0 and continuing the we get $\epsilon_0 2 \dots \epsilon_0 \omega \dots \epsilon_0^2 \dots$

• ordinal numbers that are not finite are called transfinite

• if two ordinal numbers are similar then they are equal.

• each element of an ordinal number is at the same time a subset of the ordinal number

• each initial segment of an ordinal number is an ordinal number.

• two ordinal numbers are similar or one is similar to an initial segment of another so given two ordinal numbers they are equal or one belongs to another (or subset of another).

• every set of ordinal numbers has a supremum (namely the union of each of them) which is an ordinal number.

• from above point we get : there cannot be a set of all ordinal numbers.

• **Counting Theorem** : Each well ordered set is similar to a unique ordinal number.

5.1 Arithmetic of ordinal numbers

• any collection of sets E_i can be made disjoint by defining corresponding similar sets $\hat{E_i} = E_i \times \{i\}$ so considering only disjoint sets for operations makes sense for all the operations below.

• for order in $E \cup F$ (E, F are disjoint sets with order relation R, S) we take the ordered pair set $R \cup S \cup (E \times F)$ as the defining the new order. This is called ordinal sum

• if α and β are ordinal numbers then $\alpha + \beta$ is the ordinal number of set formed by ordinal sum of sets whose ordinal numbers are α and β i.e if $\mathbf{ord}(A)$ denotes the ordinal number of set A then sum $\alpha + \beta$ is equal to $\mathbf{ord}(C) = \mathbf{ord}(A) + \mathbf{ord}(B)$ for $\mathbf{ord}(A) = \alpha, \mathbf{ord}(B) = \beta$ and C is the ordinal sum of A and B.

• properties:

$$\alpha + 0 = 0 + \alpha = \alpha$$
$$\alpha + 1 = \alpha^+$$
associative law holds
commutative law does not hold

(eg: $1 + \omega = \omega$ (as adding a distinct element to set ω in the beginning doesnt change ω) but $\omega + 1 = \omega^+ \neq \omega$ (as adding a adding distinct element to set ω in the end makes it have a supremum element))

5.2 Ordinal product

• if A and B are two well ordered sets then define $A_b = A \times b$ for $b \in B$ then ordinal product of sets can be formulated by sets $\{A_b\}$ as Cartesian product $A \times B$ with order $(a, b) < (c, d)$ means either $b < d$ or $b = d$ and $a < c$

• product of ordinal numbers is equal to the ordinal number of the ordinal product of corresponding sets having the ordinal number.

• properties

$$\alpha 0 = 0\alpha = 0$$
$\alpha 1 = 1\alpha = \alpha$ associative law holds
commutative law fails $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$
right distribution law fails

(eg: $2\omega = \omega$ (this is same as infinite sequence of ordered pair) but $\omega 2 \neq \omega$ (this is same

as ordered pair of infinite sequences)), $2\omega = (1+1)\omega = \omega + \omega = \omega 2$ (right distribution fails)

6 Cardinal numbers

• For sets X, Y if X is equivalent to a subset of Y then $X \lesssim Y$ denote this

• **Schroder-Bernstein Theorem** : $X \lesssim Y$ and $Y \lesssim X \iff X \sim Y$

• Clearly $\lesssim$ has essential properties of partial order

• **comparability theorem of sets** : if X and Y are sets the $X \lesssim Y$ or $Y \lesssim X$

• let $X \prec Y$ mean $X \lesssim Y$ and X is not equivalent to Y

• a set X is countable if $X \lesssim \omega$ or $X \sim \omega$ (countably infinite)

• **Cantor's theorem** : $X \prec P(X)$ for every set X

• a cardinal number is an ordinal number α such that if β is an ordinal number equivalent to α then $\alpha \leq \beta$

• ordinal number of a set is not unique (it changes with the order)(eg if in the set ω we to be order it to have 1 as a supremum, and all others elements with same ordering as in ω then ordinal number of this new well ordered set is ω^+)

• let cardinal number of the set X (= $card(X)$)be the least ordinal number it is equivalent to (this is possible as we can well order a set of ordinal numbers)

• $card(X) = card(Y) \iff X \sim Y$

6.1 Cardinal arithmetic

• If A and B are disjoint sets, $card(A) = a$ and $card(B) = b$ the $a + b = card(A \cup B)$ this defines addition of cardinal numbers

• cardinal addition obeys most laws of ordinary addition

• $a.b = card(A \times B)$ defines cardinal multiplication

• this too obeys most laws

• now if a is finite and b is infinite then $a + b = b$, $b + b = b$ and $b.b = b$

• since ordering of ordinal numbers is same as that for cardinal numbers we cannot have a largest cardinal number nor the set of all cardinal numbers

• $a < 2^a$ for any cardinal number

• the smallest transfinite ordinal number is the cardinal number of set ω it is denoted by $\aleph_0$

• clearly $\aleph_0 < 2^{\aleph_0}$

• every arithmetic operations of ω gives a countable ordinal number.

• let the least uncountable ordinal number be the cardinal number $\aleph_1$

• clearly $\aleph_1 \leq 2^{\aleph_0}$

• **Continuum hypothesis** : There are no cardinal number between $\aleph_0$ and $2^{\aleph_0}$ i.e. $\aleph_1 = 2^{\aleph_0}$

References

[1] Paul R. Halmos: Naive Set Theory, (1960)