Notes on Set Theory

1 Introduction

- **Extensionality Property**: A set is determined by its members
$$A = B \iff (\forall x)[x \in A \Leftrightarrow x \in B]$$
- A **function** $f : X \to Y$ associates with each member x of the set X some member $f(x)$ of Y. $(x \mapsto f(x))$ is a name-free notation for functions.
  - f is an **injection** (one-to-one) if
  $$(\forall x, y \in X)[f(x) = f(y) \Rightarrow x = y]$$
  - f is a **surjection** (onto) if
  $$(\forall y \in Y)(\exists x \in X)[f(x) = y]$$
  - f is a **bijection** (correspondence) if
  $$(\forall y \in Y)(\exists! x \in X)[f(x) = y]$$
- Given a set A, the **identity function** on A, I_A, is the total function $(x \mapsto x)$.
- A function $f : A \to B$ is *surjective* iff there exists a (total) function $g : B \to A$ s.t. $g \circ f = I_B$.
- If there exists a (total) function $g : B \to A$ s.t. $f \circ g = I_A$ then $f : A \to B$ is *injective*.
- If $f : A \to B$ is injective and $A \neq \varnothing$ then there exists a function $g : B \to A$ s.t. $f \circ g = I_A$.
- A function $f : A \to B$ is *bijective* iff there exists a unique function f^{-1} s.t. $f \circ f^{-1} = I_A$ and $f^{-1} \circ f = I_B$; f^{-1} is called the **inverse** of f.
- For every $f : X \to Y$ and $A \subseteq X$, the set
$$f[A] = \{f(x) : x \in A\}$$
is the **image of** A **under** f, and if $B \subseteq Y$, then
$$f^{-1}[B] = \{x \in X : f(x) \in B\}$$
is the **pre-image of** B **by** f.

2 Equinumerosity

- Two sets A, B are **equinumerous** if there exists a (one-to-one) *correspondence* between their elements, i.e.,
$$A =_c B \triangleq (\exists f)[f : A \to_{\text{bij}} B]$$
- The set A is **less than or equal to** B **in size** if it is equinumerous with some subset of B, i.e.,
$$A \leq_c B \triangleq (\exists C \subseteq B)[A =_c C]$$
  - $A \leq_c B \Leftrightarrow (\exists f)[f : A \to_{\text{inj}} B]$
- A set A is **finite** if there exists some natural number $n \in \mathbb{N}$ such that
$$A =_c \{i : i < n\} = \{0, 1, \cdots, n-1\},$$
otherwise, A is **infinite**.
  - A set A is **Dedekind-infinite** if there exists an injection
  $$f : A \to_{\text{inj}} B \subsetneq A$$
  from A into a proper subset $B \subsetneq A$.
- A set A is **countable** if it is *finite* or *equinumerous with the set of natural numbers* $\mathbb{N}$, otherwise **uncountable**.
  - A set A is *countable* iff $A = \varnothing$ or A has an *enumeration*, where an **enumeration** is a surjection $\pi : \mathbb{N} \to_{\text{surj}} A$.
  - If A is countable and there exists an injection $f : B \to_{\text{inj}} A$, then B is also countable.
- (**Cantor's first diagonal method**) For each sequence[1] $A_0, A_1, \cdots$ of *countable* sets, the *union*
$$A = \bigcup_{i=0}^{\infty} A_i = A_0 \cup A_1 \cup \cdots$$
is also a *countable* set.
  - This technique is also called *dovetailing*, which is heavily used in computability proofs.
  - The set $\mathbb{Z}$ of integers is countable.
  - The set $\mathbb{Q}$ of rational numbers is countable.
    - Since
    $$\mathbb{Q}^+ = \bigcup_{n=1}^{\infty} \left\{ \frac{m}{n} : m \in \mathbb{N} \right\},$$
    and each $\{m/n : m \in \mathbb{N}\}$ for fixed n is countable, $\mathbb{Q}^+$ is countable. $\mathbb{Q}^-$ is countable similarly.
- (**Cantor's second diagonal method**) The set of *infinite*, binary sequences
$$\Delta = \{(a_0, a_1, \cdots) : (\forall i)[a_i = 0 \vee a_i = 1]\}$$
is uncountable.
  - The set $\mathbb{R}$ of real numbers is uncountable.
  - The set of total functions on $\mathbb{N}$ is uncountable.
- If $A_1, \cdots, A_n$ are all countable, so is their Cartesian product $A_1 \times \cdots \times A_n$.
  - For every countable set A, each A^i $(i \geq 2)$ and the union $\bigcup_{i=2}^{\infty} A^i$ is countable.
- The set $\mathcal{K}$ of *algebraic real numbers* is countable (Cantor), and hence there exists a real number that is not algebraic (Liouville).
- (Cantor) For every set A,
$$A <_c \mathcal{P}(A),$$
i.e., $A \leq_c \mathcal{P}(A)$ but not $A \neq_c \mathcal{P}(A)$, where $\mathcal{P}(A)$ is the **powerset** of A.
  - Proof of $A \leq_c \mathcal{P}(A)$: $(x \mapsto \{x\})$ is an injection from A to $\mathcal{P}(A)$.

[1] this implies an 'enumeration', which, in turn, implies the countability of the sequence

- Proof of $A \neq_c \mathcal{P}(A)$: To the contrary, let π be a correspondence between A and $\mathcal{P}(A)$ and let

$$B = \{x \in A : x \notin \pi(x)\}.$$

Since $B \subseteq A$ (i.e., $B \in \mathcal{P}(A)$), there should exist $b \in A$ such that $B = \pi(b)$, and either $b \in B$ or $b \notin B$. Both cases lead to contradiction (Russell phenomenon!).

  * *This proof is a fairly straightforward generalization of Cantor's second diagonal method.*
  * (cont.) Why? *We constructed $B \in \mathcal{P}(A)$ so that B is not equal to any element of $\mathcal{P}(A)$ using self-reference.*

- (**Schröder-Bernstein Theorem**) For any two sets A, B,

$$(A \leq_c B \ \wedge \ B \leq_c A) \Rightarrow A =_c B$$

  - $\mathcal{P}(\mathbb{N}) \leq_c \mathbb{R}$ and $\mathbb{R} \leq_c \mathcal{P}(\mathbb{N})$
  - $\mathcal{P}(\mathbb{N}) = \mathbb{R}$.

- A set A is **transitive** if every set B which is an element of A has the property that all of *its* elements also belong to A.
  - For every set $B \in A$, $B \in \mathcal{P}(A)$.
  - For every set $B \in A$, $B \subseteq A$.
  - $\bigcup A \subseteq A$.
  - For any set A, $TC(A)$ is the smallest transitive set including A; it is called the **transitive closure** of A: e.g.,

$$TC(A) = \bigcup \{A, \bigcup A, \bigcup\bigcup A, \cdots\}.$$

3 Paradoxes and Axioms

- (**Hypothesis of Cardinal Comparability**) For any two sets A, B, either $A \leq_c B$ or $B \leq_c A$.
- (**Continuum Hypothesis; CH**) There is no set of real numbers X with cardinality intermediate between those of $\mathbb{N}$ and $\mathbb{R}$, i.e.,

$$(\forall X \subseteq \mathbb{R})[X \leq_c \mathbb{N} \ \vee \ X =_c \mathbb{R}]$$

- (**Generalized Continuum Hypothesis; GCH**) For every infinite set A,

$$(\forall X \subseteq \mathcal{P}(A))[X \leq_c A \ \vee \ X =_c \mathcal{P}(A)]$$

- (**General Comprehension Principle**) For each n-ary *definite condition P*, there is a set

$$A = \{\vec{x} : P(\vec{x})\}$$

whose members are precisely all the n-tuples of objects which satisfy $P(\vec{x})$, such that for all $\vec{x}$,

$$\vec{x} \in A \Leftrightarrow P(\vec{x})$$

  - By *extensionality principle*, only **one** set A can satisfy the above equivalence, we call this A the **extension** of the *condition P*.
  - A n-ary **condition** P is **definite** if for each n-tuple of objects $\vec{x} = (x_1, \cdots, x_n)$, it is determined 'unambiguously' whether $P(\vec{x})$ is true or false.
  - *Note that we do not demand of a definite condition that its truth value be* effectively decidable (Turing-decidable or recursive).
  - A n-ary **operation** F is **definite**, if it assigns to each n-tuple of objects $\vec{x}$ a unique, unambiguously determined object $w = F(\vec{x})$.
  - *Note again that we don't demand of a definite operation be* effectively computable.

- (**Russell's Paradox**) *The General Comprehension Principle is not valid.*
  - Russell's normal set

$$R = \{x : x \text{ is a set and } x \notin x\}$$

  - Is $R \in R$ or $R \notin R$?

Axiomatic set theory

- Zermelo's **axiomatic set theory** saved the Cantor's paradise.
- **Axiomatic setup**
  - assumption of a **domain** or **universe $\mathcal{W}$ of objects**, *including* **sets**
  - **definite conditions** and **definite operations on $\mathcal{W}$** *including **identity**, **sethood**, and **memebersip***
  - We call the objects that are not sets **atoms**; but we do not require that any atoms exist.
- (**I: Axiom of Extensionality**) For any two sets A, B,

$$A = B \ \Leftrightarrow \ (\forall x)[x \in A \ \Leftrightarrow \ x \in B]$$

- (**II: Emptyset and Pairset Axioms**)
  (a) There is a special object $\varnothing$, which is a set with no members.
  (b) For any two objects x, y, there is a set A whose only members are x and y, i.e.,

$$t \in A \ \Leftrightarrow \ t = x \text{ or } t = y$$

- (**III: Separation Axiom; Axiom of Subsets**) For each set A and each unary, definite condition P, there exists a set B which satisfies the equivalence

$$x \in B \ \Leftrightarrow \ x \in A \text{ and } P(x)$$

  - From the Extensionality Axiom, only one B satisfies the above equivalence, which we will denote by $B = \{x \in A : P(x)\}$.
  - *This axiom restricts the General Comprehension Principle and frees us from the Russell's Paradox.*

- (**IV: Powerset Axiom**) For each object A, there exists a set B whose members are the subsets of A, i.e.,

$$X \in B \ \Leftrightarrow \ Set(X) \text{ and } X \subseteq A$$

- $X \subseteq A \triangleq (\forall t)[t \in X \Rightarrow t \in A]$
- $\mathcal{P}(A) \triangleq \{X : Set(X) \text{ and } X \subseteq A\}$

- (**V: Unionset Axiom**) For every object $\mathcal{E}$, there exists a set B whose members are the members of the members of $\mathcal{E}$, i.e., it satisfies the equivalence,

$$t \in B \iff (\exists X \in \mathcal{E})[t \in X]$$

- (**VI: Axiom of Infinity**) There exists a set I which contains the empty set $\varnothing$ and the singleton of each of its members, i.e.,

$$\varnothing \in I \text{ and } (\forall x)[x \in I \Rightarrow \{x\} \in I]$$

  - In the 19th century, there was a belief that the existence of natural numbers could be proved. But now we know better: *Logic can codify the valid forms of reasoning but it cannot prove the existence of anything, let alone infinite sets.*

- For every unary, definite condition P there exists a **class**

$$A = \{x : P(x)\}$$

  such that for every object x,

$$x \in A \iff P(x)$$

  - Every set will be a class; but because of the Russell Paradox, *there must be more classes than sets.*
  - A unary definite condition P is **coextensive** with a set A if the objects which satisfy it are precisely the members of A.

$$P =_e A \triangleq (\forall x)[P(x) \Leftrightarrow x \in A]$$

  - By Russell Paradox we know that *not every P is coextensive with a set.*
  - A class is either a set or a unary definite condition which is not coextensive with a set.

- (**VII: Axiom of Choice**)
- (**VIII: Axiom of Replacement**)
- **Principle of Purity**: "Every object is a set; there are no atoms."

4 Are Sets All There Is?

- In analytic geometry the geometric line Π is "identified" with real numbers $\mathbb{R}$. The correspondence $P \mapsto x(P)$ gives a **faithful representation** of Π in $\mathbb{R}$.
- *"Now let's codify ordered pairs, relations, functions, equinumerosity, $\cdots$ in the framework of set theory."*
- Representation of **ordered pair** in **sets**
  - Characteristic properties of ordered pairs
    (a) $(x, y) = (x', y') \iff x = x'$ and $y = y'$
    (b) $A \times B \triangleq \{(x, y) : x \in A \text{ and } y \in B\}$ is a set.

- The **Kuratowski pair** operation

$$(x, y) \triangleq \{\{x\}, \{x, y\}\}$$

  satisfies above two properties.

  - *Proof of* (b): The condition

$$OrdPair_{A,B}(z) \triangleq (\exists x \in A)(\exists y \in B)[z = (x, y)]$$

  is evidently *definite*. Now if we can find for each A, B some set C such that

$$x \in A \text{ and } y \in B \Rightarrow (x, y) \in C,$$

  then, using C, we can construct a Cartesian set

$$A \times B \triangleq \{z \in C : OrdPair_{A,B}(z)\}$$

  as a set by the *Separation Axiom*. We let $C = \mathcal{P}(\mathcal{P}(A \cup B))$ since

$$\begin{aligned} x \in A, y \in B \quad &\Rightarrow \quad \{x\}, \{x, y\} \subseteq (A \cup B) \\ &\Rightarrow \quad \{x\}, \{x, y\} \in \mathcal{P}(A \cup B) \\ &\Rightarrow \quad \{\{x\}, \{x, y\}\} \subseteq \mathcal{P}(A \cup B) \\ &\Rightarrow \quad \{\{x\}, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(A \cup B)) \end{aligned}$$

- Representation of **disjoint union** in sets:

$$A \uplus B \triangleq (blue \times A) \cup (red \times B),$$

  where

$$blue \triangleq \varnothing \text{ and } red \triangleq \{\varnothing\}.$$

- A **binary relation** on the sets A, B is any subset of the Cartesian product $A \times B$.

$$xRy \triangleq (x, y) \in R.$$

  - The obvious way to represent binary relations in sets is to *identify it with its* extension*, te set of pairs which satisfy it.*

- *Every relation determines a definite condition but the converse is not true.*
  - Definite conditions $x = y$, $x \in y$, and $X \subseteq Y$ are not binary relations according to the above definition.
  - Instead, *when restricted to some set A, identity, membership*, and *subsethood* are indeed binary relations.

$$\begin{aligned} x =_A y \quad &\triangleq \quad x \in A \text{ and } y \in A \text{ and } x = y \\ x \in_A y \quad &\triangleq \quad x \in A \text{ and } y \in A \text{ and } x \in y \\ X \subseteq_A Y \quad &\triangleq \quad X \subseteq Y \subseteq A \end{aligned}$$

- A **function** (or **mapping** or **transformation**) $f : A \to B$ with *domain* the set A and *range* the set B is any subset $f \subseteq (A \times B)$ which satisfies the condition

$$(\forall x \in A)(\exists! y \in B)[(x, y) \in f].$$

  - $(A \to B) \triangleq \{f \subseteq A \times B : f : A \to B\}$: a set of all functions from A to B.
  - When A and B are sets, the set of *total* functions from A to B is sometimes denoted by

$$B^A = \{f : f \text{ is a total function from } A \text{ to } B\}$$

where $|B^A| = |B|^{|A|}$. An interesting isomorphic interpretation of B^A is the set of $|A|$-ary number with $|B|$ digits. For example, let $A = \{1, 2, \cdots, n\}$. Then

$$B^{\{1,2,\cdots,n\}} = \{(b_1, \cdots, b_n) : b_i \in B\}.$$

That is, $B^{\{1,2,\cdots,n\}}$ can be thought of as a set of *strings over A whose length is n*. Note that $(b_1, \cdots, b_n) \in B^{\{1,2,\cdots,n\}}$ denotes 'a' function f such that

$$\begin{aligned} f(1) &= b_1, \\ f(2) &= b_2, \\ &\cdots \\ f(n) &= b_n. \end{aligned}$$

- An **indexed family of sets** is a function

$$A = (i \mapsto A_i)_{i \in I} : I \to E$$

for some $I \neq \varnothing$ and some E, where each A_i is a set.

  - **union** and **intersection** of an indexed family of sets

$$\begin{aligned} \bigcup_{i \in I} A_i &\triangleq \{x \in \bigcup E : (\exists i \in I)[x \in A_i]\} \\ \bigcap_{i \in I} A_i &\triangleq \{x \in \bigcup E : (\forall i \in I)[x \in A_i]\} \end{aligned}$$

  - **product** of an indexed family

$$\prod_{i \in I} A_i \triangleq \{f : I \to \bigcup_{i \in I} A_i : (\forall i \in I)[f(i) \in A_i]$$

  - brand-new definition of **equinumerosity** and **size comparison**

$$\begin{aligned} A =_c B &\triangleq (\exists f)[f : A \to_{\text{bij}} B] \\ &\Leftrightarrow (A \to_{\text{bij}} B) \neq \varnothing \\ A <_c B &\triangleq (\exists f)[f : A \to_{\text{inj}} B] \\ &\Leftrightarrow (A \to_{\text{inj}} B) \neq \varnothing \end{aligned}$$

- For each $X \subseteq A$, the **restriction** $f \upharpoonright X$ of a function $f : A \to B$ is obtained by cutting f down so it is defined only on X,

$$f \upharpoonright X \triangleq \{(x, y) \in f : x \in X\}$$

- The basic condition of **functionhood**

$$Function(f) \triangleq (\exists A)(\exists B)[f \in (A \to B)]$$

is a definite condition.

Cantor's Notion of Cardinal Numbers

- (**Problem of Cardinal Assignment**) Define an operation $|\cdot|$ on the class of sets which satisfies

  (a) $A =_c |A|$

  (b) $A =_c B \Leftrightarrow |A| = |B|$

  (c) for each $\mathcal{E}$, $\{|X| : X \in \mathcal{E}\}$ is a set

- A (**weak**) **cardinal assignment** is any definite operation $|\cdot|$ which satisfies the conditions (a) and (c) given above. The **cardinal numbers** (relative to $|\cdot|$) are its values,

$$Card(\kappa) \Leftrightarrow \kappa \in Card \triangleq (\exists A)[\kappa = |A|].$$

A cardinal assignment $|A|$ is **strong**, if in addition, for any two cardinal numbers κ, λ,

$$\kappa =_c \lambda \Leftrightarrow \kappa = \lambda$$

which is equivalent to the condition (b) above.

- Arithmetic operations on cardinal numbers

$$\begin{aligned} \kappa + \lambda &\triangleq |\kappa \uplus \lambda| =_c \kappa \uplus \lambda \\ \kappa \cdot \lambda &\triangleq |\kappa \times \lambda| =_c \kappa \times \lambda \\ \kappa^\lambda &\triangleq |(\kappa \to \lambda)| =_c (\kappa \to \lambda) \end{aligned}$$

  - Infinitary operations may be defined similarly:

$$\sum_{i \in I} \kappa_i \triangleq \left| \left\{ (i, x) \in I \times \bigcup_{i \in I} \kappa_i : x \in \kappa_i \right\} \right|$$

and

$$\prod_{i \in I} \kappa_i \triangleq \left| \prod_{i \in I} \kappa_i \right|$$

- For every indexed family of sets $A = (i \mapsto A_i)_{i \in I}$, there exists a function $f : I \to f[I]$ s.t.

$$f(i) = |A_i| \quad (i \in I)$$

Structured Sets

- A **topological space** is a set X of points endowed with a **topological structure**, which is determined by a collection $\mathcal{T}$ of subsets of X satisfying the following three properties:

  (a) $\varnothing \in \mathcal{T}$ and $X \in \mathcal{T}$

  (b) $A, B \in \mathcal{T} \Rightarrow A \cap B \in \mathcal{T}$

  (c) For every family $\mathcal{E} \in \mathcal{T}$ of sets in $\mathcal{T}$, the unionset $\bigcup \mathcal{E}$ is also in $\mathcal{T}$.

- A family of sets $\mathcal{T}$ with the three properties is called a **topology** on X, with **open sets** its members and **closed sets** the complements of open sets relative to X, i.e., all $X \setminus G$ with G open.

- A **structured set** is a pair $U = (A, \mathcal{S})$ where $A = Field(U)$ is a set, the **field** or **space** of U, and $\mathcal{S}$ is an arbitrary object, the **frame** of U.

  - A *topological space* is a structured set $(X, \mathcal{T})$.

  - A *group* is a structured set $U = (G, (e, \cdot)) = (G, e, \cdot)$ where $e \in G$ and $\cdot : G \times G \to G$ is a binary function satisfying the group axioms.

5 The Natural Numbers

- A **system of natural numbers** is any structured set $(\mathbb{N}, 0, S) = (\mathbb{N}, (0, S))$ which satisfies the following conditions (or **axioms of Peano**):
  (a) $0 \in \mathbb{N}$
  (b) $S : \mathbb{N} \to \mathbb{N}$
  (c) S is an injection, i.e., $Sn = Sm \Rightarrow n = m$
  (d) $(\forall n \in \mathbb{N})[Sn \neq 0]$
  (e) (**Induction principle**) for each $X \subseteq \mathbb{N}$,
  $$[0 \in X \text{ and } (\forall n \in \mathbb{N})[x \in X \Rightarrow Sn \in X]] \Rightarrow X = \mathbb{N}$$
- In a system of natural numbers $(\mathbb{N}, 0, S)$, every element $n \neq 0$ is a successor,
  $$n \neq 0 \Rightarrow (\exists m \in \mathbb{N})[Sm = n]$$
  and for each n, $Sn \neq n$.
- (**Existence Theorem for the Natural Numbers**) There exists at least one system of natural numbers $(\mathbb{N}, 0, S)$.
  - Can be proved using the *Axiom of Infinity*.
- (**Uniqueness Theorem for the Natural Numbers**) For any two systems of natural numbers $(\mathbb{N}_1, 0_1, S_1)$ and $(\mathbb{N}_2, 0_2, S_2)$, there exists exactly one bijection (or **isomorphism**) $\pi : \mathbb{N}_1 \to_{\text{bij}} \mathbb{N}_2$ s.t.
  $$\begin{aligned} \pi(0_1) &= 0_2 \\ \pi(S_1 n) &= S_2 \pi(n) \quad (n \in \mathbb{N}_1) \end{aligned}$$
- (**Recursion Theorem**) Assume that $(\mathbb{N}, 0, S)$ is a system of natural numbers, E is some set, $a \in E$, and $h : E \to E$ is some function. It follows that there exists exactly one function $f : \mathbb{N} \to E$ which satisfies the identities
  $$\begin{aligned} f(0) &= a, \\ f(Sn) &= h(f(n)), \quad (n \in \mathbb{N}) \end{aligned}$$
  - *The Recursion Theorem justifies the usual way by which we can define functions on the natural numbers by recursion (or induction)*
  - From a purely mathematical view, Recursion Theorem can be viewed as a theorem of *existence and uniqueness of solutions of the system of the identities where f is the unknown*.
  - Recursion Theorem is a special case of **Continuous Least Fixed Point Theorem**, which, in turn, is a special case of **Fixed Point Theorem** of Zermelo.
- (**Recursion with parameters**) For any two sets Y, E and functions
  $$g : Y \to E, \quad h : E \times Y \to E,$$
  there exists exactly one function $f : \mathbb{N} \times Y \to E$ which satisfies the identities
  $$\begin{aligned} f(0, y) &= g(y) \quad (y \in Y), \\ f(n+1, y) &= h(f(n, y), y) \quad (y \in Y, n \in \mathbb{N}) \end{aligned}$$

The Natural Numbers

- We denote the cardinal number of $\mathbb{N}$ by the first Hebrew letter,
  $$\aleph_0 \triangleq |\mathbb{N}|$$
- Functions $a : \mathbb{N} \to A$ with the domain $\mathbb{N}$ are called (infinite) **sequences** and we often write their argument as a subscript,
  $$a_n = a(n) \quad (n \in \mathbb{N}, a : \mathbb{N} \to A)$$
- *Addition and multiplication.* The addition function on the natural numbers is defined by the recursion
  $$\begin{aligned} n + 0 &= n, \\ n + Sm &= S(n + m) \end{aligned}$$
  and multiplication is defined next, using addition, by the recursion
  $$\begin{aligned} n \cdot 0 &= 0, \\ n \cdot Sm &= (n \cdot m) + m \end{aligned}$$
- A binary relation $\leq$ on a set P is a **partial ordering** if it is reflexive, transitive, and antisymmetric.
- The partial ordering $\leq$ is **total** (or **linear**) if any two elements of P are **comparable** in $\leq$, i.e.,
  $$(\forall x, y \in P)[x \leq y \text{ or } y \leq x]$$
- The binary relation $\leq$ on P is a **wellordering** of P if it is a total ordering of P and, in addition, *every non-empty subset of P has a least element*,
  $$(\forall X \subseteq P)[X \neq \varnothing \Rightarrow (\exists x \in X)(\forall y \in X)[x \leq y]$$
  - The order relation $\leq$ on the natural numbers is defined by the equivalence
  $$n \leq m \triangleq (\exists s)[m = n + s]$$
  - The ordering $\leq$ on $\mathbb{N}$ is a wellordering.
- A set A is **finite** if there exists some natural number n s.t. $A =_c [0, n)$, **infinite** if it is not finite and **countable** if it is finite or equinumerous with $\mathbb{N}$. The **finite cardinals** are the cardinal numbers of finite sets.
- (**Pigeonhole Principle**) Every injection $f : A \to_{\text{inj}} A$ on a finite set into itself is also a surjection, i.e. $f[A] = A$.
- (**Simultaneous Recursion Theorem**) For each two sets E_1, E_2, elements $a_1 \in E_1, a_2 \in E_2$, and functions $h_1 : E_1 \times E_2 \to E_1, h_2 : E_1 \times E_2 \to E_2$, there exists unique functions
  $$f_1 : \mathbb{N} \to E_1, \quad f_2 : \mathbb{N} \to E_2$$
  which satisfy the identities
  $$\begin{aligned} f_1(0) &= a_1, \\ f_2(0) &= a_2, \\ f_1(n+1) &= h_1(f_1(n), f_2(n)), \\ f_2(n+1) &= h_2(f_1(n), f_2(n)) \end{aligned}$$

The Cardinal Numbers

- For each set A, we define the set of **finite sequences** (or **words** or **strings**) from A by

$$\begin{aligned} A^{(n)} &\triangleq \{u \in \mathbb{N} \times A : \textit{Function}(u) \text{ and } \textit{Domain}(u) = [0, n)\}, \\ A^* &\triangleq \bigcup_{i=0}^{\infty} A^{(i)} \end{aligned}$$

  - The **length** of the string u is defined as

$$lh(u) \triangleq \max\{i : i = 0 \text{ or } i - 1 \in \textit{Domain}(u)\},$$

    $u \in A^*$

  - We let $u \sqsubseteq v$ if $u \subseteq v$ for $u, v \in A^*$ and we call u an **initial segment** of v if $u \sqsubseteq v$.

- For each cardinal number κ and each $n \in \mathbb{N}$, we set

$$\kappa^n \triangleq |\kappa^{(n)}|$$

- For each countably infinite set A and each $n > 0$,

$$A =_c A \times A =_c A^{(n)} =_c A^*.$$

  As equations of cardinal arithmetic, these read:

$$\aleph_0 =_c \aleph_0 \cdot \aleph_0 =_c {\aleph_0}^n =_c |\aleph_0^*|$$

- The Continuum. The classical notation for the cardinal of $\mathcal{P}(\mathbb{N})$ is

$$\mathfrak{c} \triangleq |\mathcal{P}(\mathbb{N})| =_c 2^{\aleph_0}$$

  - $\mathfrak{c} \cdot \mathfrak{c} =_c 2^{\aleph_0} \cdot 2^{\aleph_0} =_c 2^{\aleph_0 + \aleph_0} =_c 2^{\aleph_0} =_c \mathfrak{c}$
  - $\mathfrak{c} =_c {\aleph_0}^{\aleph_0} =_c \mathfrak{c}^{\aleph_0}$
  - *The Continuum Hypothesis* revisited

$$(\forall \kappa \leq_c \mathfrak{c})[\kappa \leq_c \aleph_0 \text{ or } \kappa =_c \mathfrak{c}]$$

6 Fixed Points

- A **partially ordered set** (or **poset**) is a structured set

$$P = (\textit{Field}(P), \leq_P),$$

  where *Field*(P) is an arbitrary set and $\leq_P$ is a partial ordering on *Field*(P).

  - Note that $\leq_P$ determines P since it's reflexive, i.e.

$$x \in \textit{Field}(P) \Leftrightarrow x \leq_P x$$

  - $\bot = \bot_P \triangleq$ the least element of P (if it exists)

- Let P be a poset, $S \subseteq P$ and $M \in P$ a member of P.

  1. M is an **upper bound** of S if it is greater than or equal to every element of S, i.e. $(\forall x \in S)[x \leq M]$.
  2. M is a **greatest element** in S if it is a member and an upper bound of S, i.e. $M \in S$ and $(\forall x \in S)[x \leq M]$.
  3. M is a **least upper bound** of S if it is an upper bound and also less than or equal to every other upper bound of S, i.e.

$$(\forall x \in S)[x \leq M]$$

     and

$$(\forall M')[(\forall x \in S)[x \leq M'] \Rightarrow M \leq M']$$

  4. M is **maximal** in S if

$$(\forall x \in S)[M \leq x \Rightarrow M = x].$$

     Note that maximal elements are not necessarily unique.

- When it exists, the least upper bound of S is denoted by

$$\sup S = \text{ the least upper bound of } S$$

  - There exists *at most one* least upper bound of S.
  - If M is a greatest element of S then M is the least upper bound of S.

- A **partial function** on a set A to a set E is any function with domain of definition some subset of A and values in E, in symbols

$$\begin{aligned} f : A \rightharpoonup E \quad &\triangleq \quad \textit{Function}(f) \text{ and} \\ &\qquad \textit{Domain}(f) \subseteq A \text{ and } \textit{Image}(F) \subseteq E \end{aligned}$$

  - $(A \rightharpoonup E) \triangleq \{f \subseteq A \times E : f : A \rightharpoonup E\}$

- A **chain** in a poset P is any linearly ordered subset S of P, i.e. a subset satisfying

$$(\forall x, y \in S)[x \leq y \text{ or } y \leq x].$$

  A poset P is **chain-complete** or **inductive** if every chain in P has a *least upper bound*.

  - For each set A, the powerset $\mathcal{P}(A)$ is inductive.
  - For any two sets A, B, the poset $(A \rightharpoonup E)$ of all partial functions from A to E is inductive.
  - For every poset P, the set

$$\textit{Chains}(P) \triangleq \{S \subseteq P : S \text{ is a chain}\}$$

    of all chains in P (partially ordered under $\subseteq$) is inductive.

- (**Zorn's Lemma**) Given a poset $(P, \leq_P)$, if every nonempty chain has an upper bound, then P has at least one greatest element.

- A mapping $\pi : P \to Q$ on a poset P to another is **monotone** if for all $x, y \in P$,

$$x \leq_P y \Rightarrow \pi(x) \leq_Q \pi(y)$$

- A monotone mapping $\pi : P \to Q$ on an *inductive* poset to another is **countably continuous** if for every non-empty, countable chain $S \subseteq P$,

$$\pi(\sup S) = \sup \pi[S]$$

- (**Continuous Least Fixed Point Theorem**) Every countably continuous, monotone mapping $\pi : P \to P$ on an inductive poset into itself has exactly one **strongly least fixed point** x^*, which is characterized by the two properties,

$$\pi(x^*) = x^*,$$
$$(\forall y \in P)[\pi(y) \le y \Rightarrow x^* \le y]$$

- A partial function $g : A \rightharpoonup E$ is **finite** if it has finite domain, i.e. if it is a finite set of ordered pairs. A mapping $\pi : (A \rightharpoonup E) \to (B \rightharpoonup M)$ from one partial function space to another is **continuous**, if it is monotone and for each $f : A \rightharpoonup E$, and each $y \in B$ and $v \in M$,

$$\pi(f)(y) = v \Rightarrow (\exists g \in f)[g \text{ is finite and } \pi(g)(y) = v]$$

  - A function $f : X \to Y$ from one topological space to another is (topologically) **continuous** if the inverse image $f^{-1}[G]$ of every open subset of Y is an open subset of X.

- Every continuous mapping $\pi : (A \rightharpoonup E) \to (B \rightharpoonup M)$ is countably continuous, in fact, for every (not necessarily countable) non-empty chain $S \subseteq (A \rightharpoonup E)$,

$$\pi(\sup S) = \sup \pi[S]$$

7 Well-Ordered Sets

- A **well-ordered set** is a poset

$$U = (\mathit{Field}(U), \le_U),$$

  where $\le_U$ is a **wellordering** on $\mathit{Field}(U)$, i.e. a linear (total) ordering on $\mathit{Field}(U)$ such that every non-empty $X \subseteq \mathit{Field}(U)$ has a least member.

  - Associated with U is also its **strict ordering** $<_U$,

$$x < y \iff x <_U y \triangleq x \le_U y \text{ and } x \neq y.$$

- A set is **well orderable** if it admits a wellordering, so it is the field of some well ordered set $(A, \le)$.

  - One important lesson in this section is that *well orderable sets behave much better than arbitrary sets, for example, any two of them are comparable in cardinality*.
  - If fact, *every set is well orderable*, which was proved by Zermelo.

References

[1] J. Barwise, editor. *Handbook of Mathematical Logic*. North Holland, 1977.

[2] J. Barwise and L. Moss. *Vicious Circles*. CSLI Publications, 1996.

[3] Y. N. Moschovakis. *Notes on Set Theory*. Springer Verlag, 1994.