Axiomatic Set Theory, Functions, and Numbers

Taghi Farzad

University of California, Riverside

September, 2018

Set Theory

- Sets are collections of objects. A set is a single entity. (Similar to a box)
- The objects in a set S are called elements of S. (The balls in the box)
- We write $x \in S$ to mean that x is an element of S (x is contained in S) (x belongs to S).
- We write $x \notin S$ to mean that x is not an element of S.

Set Theory

- **Russel's Paradox**: Let $R = \{x | x \notin x\}$, then $R \in R \implies R \notin R$.

- To circumvent these philosophical paradoxes, an axiomatic system has been proposed to study the Set Theory

Set Theory

1. Axiom of Extensionality: If X and Y have the same elements, then $X = Y$

$$\forall x \ (x \in X \Leftrightarrow x \in Y) \Rightarrow X = Y$$

- Example: $X = \{a, b\}$, $Y = \{a, b\}$, then $X = Y$

Set Theory

2. Axiom of the Null Set:

$$\exists ! X \ \ \forall y : \neg(y \in X)$$

- In words, there exists (a unique) empty set. (Why unique?)
- Since it is unique, let's denote it by "$\varnothing$", the *empty* set.

- $\varnothing \neq \{\varnothing\}$

$$\varnothing = \{x | x \wedge \neg x\}$$

- An empty box is not the same as nothing!
- Syllogism: Nothing is better than eternal happiness; a ham sandwich is better than nothing; therefore, a ham sandwich is better than eternal happiness!

Set Theory

3. Axiom of Pairing (Axiom of Unordered Pair): For any X and Y there exists a set that contains X and Y as elements.

$$\forall X \ \forall Y, \ \exists Z \ (X \in Z \wedge Y \in Z)$$

Set Theory

- We can specify sets by listing all of its elements, i.e. $A = \{a, b, c\}$.
- We can also specify sets by the collection of objects that satisfy a certain property.

4. Axiom of Subsets (Separation or Comprehension): If φ is a property with parameter p, then for any X and p there exists a set $Y = \{x \in X | \varphi(x, p)\}$ that contains all those elements of x that have the property φ

$$\forall X, \ \forall p \ \exists Y : \quad \forall x (x \in Y \Leftrightarrow (x \in X \wedge \varphi(x, p)))$$

Set Theory: Digression

- If every element in A is also an element in B, then A is a subset of B and we write $A \subseteq B$ or $B \supseteq A$

$$\forall a(a \in A \Rightarrow a \in B) \Rightarrow A \subseteq B$$

- Example: $A = \{a, b, c\}$, $B = \{a, b, c, d, e, f\}$, $C = \{a, b, z\}$, then $A \subseteq B$, but $C \nsubseteq B$
- If $A \subseteq B$ and $B \subseteq A$, then $A = B$.
- If $A \subseteq B$ and $A \neq B$, then A is said to be a proper subset of B and we write $A \subset B$ or $B \supset A$.

Set Theory

5. Axiom of the Power Set: For any X there exists a set $Y = P(X)$, the set of all subsets of X

$$\forall X \ \exists Y \ \forall x (x \in Y \Leftrightarrow x \subseteq X)$$

- We can also write 2^S instead of $P(S)$
- Example: $S = \{a, b\}$, then $P(S) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- Example: $S = \emptyset$, then $P(S) = \{\emptyset\}$

Set Theory: Digression

- Define $|S|$ as the total number of objects in S, a set that contains finitely many elements.
- **Cardinality**: Number of elements of a set.
- If $|S| = 1$ we say that S is a singleton
- Example: $|\{a, b, c\}| = 3$, $|\emptyset| = 0$
- Clearly, $A \subseteq B \Rightarrow |A| \leq |B|$ and $A \subset B \Rightarrow |A| < |B|$

Set Theory

6. Axiom of the Sum of Sets (Union): For any X set of sets X there exists $Y = \bigcup X$, the union of all elements of X

$$\forall X \ \exists Y \ \forall x \left(x \in Y \Leftrightarrow \exists z \Big((z \in X) \wedge (x \in z) \Big) \right)$$

- Example: $X = \{\{a, b, 1\}, \{1, 2\}\}$, then $Y = \bigcup X = \{a, b, 1, 2\}$
- We usually write $A \cup B$ to mean $\bigcup \{A, B\}$
- Some properties:
  - $A \cup B = B \cup A$
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $\forall A (A \cup \emptyset = A)$

Set Theory: Digression

- Likewise one can construct intersection of sets

Theorem

Let A, B be sets. Then there exists a unique set C whose elements belong to both A and B

$$\exists! C \;\; \forall x (x \in C \Leftrightarrow x \in A \land x \in B)$$

- Again we can write $C = \bigcap\{A, B\}$ or $C = A \cap B$
- Example: $\{1, 2, 4\} \cap \{1, 2\} = \{1, 2\}$
- Some properties:
  - $A \cap B = B \cap A$
  - $A \cap (B \cap C) = (A \cap B) \cap C$
  - $\forall A (A \cap \emptyset = \emptyset)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Set Theory

7. Axiom of Infinity: There exists an infinite set

$$\exists S \left[\emptyset \in S \wedge \left[(\forall x \in S)[x \cup \{x\} \in S] \right] \right]$$

Set Theory

7. Axiom of Regularity (Foundation): Every nonempty set, S, has a member ($\in -$minimal element) that is disjoint with S:

$$\forall S[S \neq \emptyset \Rightarrow (\exists x \in S) S \bigcap x = \emptyset]$$

- This implies no set is an element of itself. (Why?)
- Evey set has an **Ordinal Rank**.

Set Theory: Digression

- We can appeal to the two above to show the existence of set of natural numbers exist
  - Let $0 := \emptyset$; $1 := \{\emptyset\}$; $2 := \{\emptyset, \{\emptyset\}\}$; $3 := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$
  - Then, the axiom of infinity tell us that the set $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ exists
  - Useful notation: We will denote $\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$

Set Theory

8. Axiom of Replacement: Given any set X and any function F defined on X ($Y = F[X] = \{F(x) : x \in X\}$), the image $F(X)$ is a set:

$$\forall x \ \ \forall y \ \ \forall z[\varphi(x, y, p) \wedge \varphi(x, y, p) \Rightarrow y = z]$$

$$\forall X \ \ \exists Y \ \ \forall y \left[y \in Y \equiv \exists x \in X \varphi(x, y, p)] \right]$$

Set Theory: Digression

- Appealing to axioms of om the axioms of pairing, union, power set, and specification one can define the unique set of **Cartesian Product**:
- Let A and B be sets. Then, there exists a unique set C such that every element of C has the form (a, b) where $a \in A$ and $b \in B$.

$$\forall A \ \forall B \ \exists! C \ \forall a \ \forall b \Big((a, b) \in C \Leftrightarrow (a \in A \wedge b \in B) \Big)$$

- Usually we write $C = A \times B$. Note: $A \times B \neq B \times A$
- Example: $\{1, 2\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b)\}$. $\{1, 2\} \times \emptyset = \emptyset$
- For any $(A_i)_{0 \leq i \leq n}$, $(n \in \mathbb{N})$ we can write the n-fold Cartesian product

$$\prod_{i=0}^{n} = A_0 \times A_1 \times \cdots \times A_n = \{(a_1, a_2, \dots a_n) | a_i \in A_i\}$$

Set Theory

9. Axiom of Choice: The Cartesian Product of a collection of non-empty sets is non-empty.

- Alternatively,
  - Every family of nonempty sets has a choice function.
  - Given any non-empty set A whose elements are pairwise disjoint non-empty sets, there exists a set B consisting of exactly one element taken from each set belonging to A.
- Axiom of Choice helps us to construct the choice functions.

Set Theory

- The system of axioms 1-7 is called Zermelo set theory, "Z",
- The system of axioms 1-8 is called Zermelo-Frankael set theory, "ZF"
- The system of axioms 1-9 is denoted by "ZFC"

Relations

- Relation: Let X, Y be sets. Then, a subset R of $X \times Y$ is called a (binary) relation from X to Y.
- If $X = Y$, then we say that R is a relation on X
- We usually write xRy instead of $(x, y) \in R$

Relations

- Properties of relations. A relation on X is said to be:
  - Reflexive if xRx holds for all $x \in X$
  - Complete (Connex)if xRy or yRx for all $x, y \in X$
  - Symmetric if $xRy \Rightarrow yRx$ for all $x, y \in X$
  - Antisymmetric if $(xRy \wedge yRx) \Rightarrow x = y$ for all $x, y \in X$
  - Asymmetric if $xRy \Rightarrow \neg(yRx)$ for all $x, y \in X$
  - Transitive if $(xRy \wedge yRz) \Rightarrow xRz$ for all $x, y, z \in X$

Relations

- **Equivalence Relation** ($\sim$): A binary relation that is reflexive, symmetric, and transitive.
  - Note the difference between $\sim$ and $=$.
- **Equivalence Class**: For any $x \in X$ the equivalence class of x relative to $\sim$ is defined as the set

$$[x]_\sim := \{y \in X | y \sim x\}$$

  - Example: indifference curves
- **Quotient Set**: The class of all equivalence classes relative to $\sim$ is denoted as $X/_\sim$ and is called the quotient set of X relative to $\sim$

$$X/_\sim := \{[x]_\sim | x \in X\}$$

  - Example: the set of all possible indifference curves

Relations

- A partition of a nonempty set X is a set of nonempty subsets of X such that every element $x \in X$ is in exactly one of these subsets
- Formally, $\mathcal{A}$ is a partition of X if

$$(\emptyset \notin \mathcal{A}) \wedge \left(\bigcup \mathcal{A} = X\right) \wedge$$

$$\left(\forall A \ \forall B \left(\left((A \in \mathcal{A}) \wedge (B \in \mathcal{A}) \wedge (A \neq B)\right) \Rightarrow A \cap B = \emptyset\right)\right)$$

Theorem

For any equivalence relation $\sim$ on a nonempty set X, the quotient set $X/_{\sim}$ is a partition of X.

- In particular, this implies, no two indifference curves intersect

Relations

- A relation $\succeq$ on a nonempty set X is called a preorder (or quasiorder) on X if it is transitive and reflexive
  - Graphs
  - $\sim$ is a symmetric preorder relation.
- A relation $\succeq$ on a nonempty set X is called a partial on X if it is an antisymmetric preorder on X.
  - Family Tree Graphs
- A relation $\succeq$ on a nonempty set X is called a a linear order (or total order) on X if it is a partial order on X and is complete.
  - Lexicographical Order

Relations

- A preordered set is a list $(X, \succeq)$, where X is a nonempty set and $\succeq$ is a preorder on X.
- A partially ordered set is a list $(X, \succeq)$, where X is a nonempty set and $\succeq$ is a partial order on X.
- A linearly ordered set is a list $(X, \succeq)$, where X is a nonempty set and $\succeq$ is a linear order on X.

Relations

- **Least Element**: $\underline{x} \in X$ is called a least element of X with respect to a linear order $\succeq$ if $x \succeq \underline{x}$ for all $x \in X$

- A well-ordered set is a totally ordered set in which every nonempty subset has a least member
- $(\mathbb{N}, >)$ is a well-ordered set but $(\mathbb{R}, >)$ and $(\mathbb{Z}, >)$ are not.

Theorem

Well-Ordering Theorem: For every set X there exists a well-ordering with domain X.

- This theorem is equivalent to the axiom of choice

Functions

- Let X and Y be sets. A relation f from X to Y, denoted by $f : X \mapsto Y$ is a function if
  (i) for every $x \in X$ there exists a $y \in Y$ such that xfy
  $$\forall x(x \in X \Rightarrow \exists y \in Y(xfy))$$
  (ii) for every $y, z \in Y$ with xfy and xfz we have $y = z$
  $$\forall y \ \forall z \ \forall x(y \in Y \wedge z \in Y \wedge x \in X \wedge xfy \wedge xfz \Rightarrow y = z)$$
- We call X the domain of f and Y the codomain of f
- The range (or image) of f is defined by $f(X) := \{y \in Y | \exists x \in X(xfy)\}$

Functions

- Recall,
  8. Axiom of Replacement: Given any set X and any function F defined on X ($Y = F[X] = \{F(x) : x \in X\}$), the image $F(X)$ is a set:

$$\forall x \ \forall y \ \forall z[\varphi(x, y, p) \wedge \varphi(x, y, p) \Rightarrow y = z]$$

$$\forall X \ \exists Y \ \forall y \left[y \in Y \equiv \exists x \in X \varphi(x, y, p)] \right]$$

- The axiom assures us that the image of any function is also a set

Functions

- If $f(X) = Y$, then we say that f maps X onto Y. We call such a function a surjection.

$$\forall y(y \in Y \Rightarrow \exists x \in X(f(x) = y))$$

- If f maps distinct points in its domain to distinct points in its codomain then we say tha f is an injection (on-to-one mapping).

$$\forall a \forall b((a \in X \wedge b \in X \wedge f(a) = f(b)) \Rightarrow a = b)$$

- If f is both surjective and injective, then we call it a bijection

Functions

- The inverse image of a set B in Y denoted as $f^{-1}(B)$ is defined as the set of all $x \in X$ whose image under f belongs to B

$$f^{-1}(B) := \{x \in X | f(x) \in B\}$$

Theorem

Let $f : X \mapsto Y$ be a function. Then, for any $y \in Y$, $f^{-1}(y)$ is a singleton if and only if f is an injection

$$(\forall y(y \in Y \wedge |f^{-1}(y)| = 1)) \Leftrightarrow$$

$$(\forall a \forall b((a \in X \wedge b \in X \wedge f(a) = f(b)) \Rightarrow a = b))$$

Functions

- For any function $f : X \mapsto Y$ we can define the set

$$f^{-1} := \{(y, x) \in Y \times X | xfy\}$$

this is a relation that maps the inverse of f. We say that f is invertible if f^{-1} is a function. We call that function f^{-1} the inverse of f

Theorem

Let $f : X \mapsto Y$ be a function. Then, $f^{-1} : Y \mapsto X$ is a function if and only if f is a bijection.

Fields

- A function of the form $\bullet : X \times X \mapsto X$ is referred to as a binary operation on X and we write $x \bullet y$ instead for $\bullet(x, y)$
  - Example: $+ : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$
  - Example: $\cdot : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$

Fields

- **Definition**: A field is a set X, along with two binary operations, $+$ and $\cdot$, denoted by $(X, +, \cdot)$ that satisfy the following properties:
  1. Commutativity:
  $$\forall x \ \forall y((x \in X \wedge y \in X) \Rightarrow (x + y = y + x \wedge xy = yx))$$
  2. Associativity:
  $$\forall x \ \forall y \ \forall z((x + y) + z = x + (y + z) \wedge (xy)z = x(yz))$$
  3. Distributivity:
  $$\forall x \ \forall y \ \forall z((x \in X \wedge y \in X \wedge z \in X) \Rightarrow (x(y + z) = xy + xz))$$
  4. Existence of identity elements:
  $$\exists 0 \ \exists 1 \ \forall x((0 + x = x = x + 0) \wedge (1x = x = x1))$$
  5. Existence of inverse elements:
  $$\forall x(x \in X \Rightarrow \exists -x \in X(x + -x = 0 = -x + x))$$
  $$\forall x(x \in X \setminus \{0\} \Rightarrow \exists x^{-1} \in X(xx^{-1} = 1 = x^{-1}x))$$

Fields

- A field $(X, +, \cdot)$ is an algebraic structure that allows for some minimal satisfactory algebraic operations possible.
- Given $+$ and $\cdot$ we define (for convenience) two other operations $- : X \times X \mapsto X$ and $\div : X \times X \setminus \{0\} \mapsto X$ such that

$$\forall x \forall y (x - y = x + -y)$$

$$\forall x \forall y (x \div y = xy^{-1})$$

- The entire arithmetic we are familiar with can be performed in an arbitrary field.
- A list $(X, +, \cdot, \geq)$ is called an ordered field if $(X, +, \cdot)$ is a field and $\geq$ is a partial order on X such that

$$\forall x \forall y \forall z ((x \geq y \Rightarrow x + z \geq y + z) \wedge ((z \geq 0 \wedge x \geq y) \Rightarrow xz \geq yz))$$

Fields

- Some useful notations:

$$X_+ := \{x \in X | x \geq 0\}$$

$$X_{++} := \{x \in X | x > 0\}$$

$$X_- := \{x \in X | 0 \geq x\}$$

$$X_{--} := \{x \in X | 0 > x\}$$

Numbers

- Recall we defined $\mathbb{N}_0$ as

$$\mathbb{N}_0 := \{0, 1, 2, \dots\}$$

- To investigate properties of natural numbers we can use Paeno's Axioms
  1. Zero is a number.
  2. If a is a number, the successor of a is a number.
  3. Zero is not the successor of a number.
  4. Two numbers of which the successors are equal are themselves equal.
  5. **Induction Axiom**: If a set X of numbers contains zero and also the successor of every number in X, then every number is in X.

Numbers

Theorem

If $D \subseteq \mathbb{N}$ such that $1 \in D$ and $\forall n(n \in D \Rightarrow n+1 \in D)$, then $D = \mathbb{N}$

- Show $11^n - 6$ is divisible by 5.
- Show
$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Numbers

- Once we have the natural numbers it is straightforward to construct the set of integers using a standard procedure.
- We shall denote this set as $\mathbb{Z} := \{\mathbb{N} \cup \{-n | n \in \mathbb{N} \wedge n + -n = 0\}\}$.
- Given $\mathbb{Z}$ it is easy to construct the rational numbers denoted as $\mathbb{Q} := \{n/m | n \in \mathbb{Z} \wedge m \in \mathbb{Z} \setminus \{0\}\}$.
- Next step: to construct real numbers, $\mathbb{R}$ (Tarski's axiomatization of the reals).
- It is straightforward to show that $(\mathbb{Q}, +, \cdot, \geq)$ and $(\mathbb{R}, +, \cdot, \geq)$ are ordered field.

Numbers

- A set $S \subseteq \mathbb{R}$ is said to be bounded above if it has an upper bound.

$$\exists b \ \forall x(x \in S \Rightarrow b \geq x)$$

- The supremum of a set $S \subseteq \mathbb{R}$ is the least upper bound of that set and is denoted by $\sup S$. That is, for any upper bound b, $\sup S \leq b$
- Similarly, the largest lower bound of a set S is called an infimum denoted by $\inf S$
- If $\sup S$ exists, it is easy to see that $\inf S = -\sup(-S)$, where $-S := \{-s | s \in S\}$
- $\sup S$ and $\inf S$ are not necessarily elements of S. Example, $(0, 1)$

Numbers

Theorem

Every nonempty subset S of $\mathbb{R}$ which is bounded from above has a supremum.

- The theorem above is sometimes stated as an axiom. It depends on how we construct the real numbers

Theorem

$$\forall x \in \mathbb{R} \exists n \in \mathbb{N} (x < n)$$

Equivalently

$$\forall x \in \mathbb{R} \exists n \in \mathbb{N} (1/n < x)$$

Numbers

- For any real numbers $a < b$ define (a, b) as

$$(a, b) := \{t \in \mathbb{R} | a < t < b\}$$

- Similarly, $[a, b]$ as

$$[a, b] := \{t \in \mathbb{R} | a \leq t \leq b\}$$

Theorem

For every $s < t$ the interval (s, t) contains infinitely many rational (countable) and infinitely many irrational numbers (uncountable).