

# Math Preliminaries

Adam Yin

A glossary reference for some basic mathematical terms which I found useful with a formal definition. [1] [2] [3]

## Glossary

**Absolute Complement** or simply, the *complement* of a set  $A$ , denoted by  $A^c$ , is the set of elements which do not belong to  $A$ .

$$A^c = \{x : x \in U, x \notin A\}$$

**Absolute Value** ( $||$ ) The **absolute value** of a real number  $x$ , denoted by  $|x|$ , is defined by

$$x = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Geometrically speaking, the absolute value of  $x$  is the distance between the point  $x$  on the real line and the origin point 0. Let  $a, b, c \in \mathbb{R}$ :

- $|a - b| = |b - a|$
- $|a| \geq 0$ , and  $|a| = 0$  iff  $a = 0$
- $|ab| = |a||b|$
- $|a + b| \leq |a| + |b|$
- $|a - b| \geq ||a| - |b||$
- $|a - c| \leq |a - b| + |b - c|$

**Anonymous Function** ( $\mapsto$ ) is denoted by the barred arrow, which goes from *input datum* to *output datum*.

**Antisymmetric** is a binary relation  $\alpha$  over a set  $S$  where no pair of distinct elements of  $S$  is related by  $\alpha$  to the other. Thus,  $\forall a, b \in S, (a\alpha b \wedge b\alpha a) \Rightarrow a = b$ .

**Associative** A binary operation  $\circ$  is said to be **associative** on a set  $\Omega$  if and only if  $\forall a, b, c \in \Omega, (a \circ b) \circ c = a \circ (b \circ c)$

To prove, let  $a, b, c$  be arbitrary but fixed elements in  $\Omega$ , compute  $(a \circ b) \circ c$  and  $a \circ (b \circ c)$  and show that  $(a \circ b) \circ c = a \circ (b \circ c)$ .

**Axiom/Postulate** is a mathematical statement that is taken to be self-evidently true without proof. These are basic building blocks from which all theorems are proved.

**Biconditional Statement** ( $\Leftrightarrow$ ) Let  $P$  and  $Q$  be statements, the **biconditional statement** is  $P$  if and only if  $Q$ , or  $P$  iff  $Q$ .

*Note:*  $P \Leftrightarrow Q$  is only true if both  $P \Rightarrow Q$  and its converse  $Q \Rightarrow P$  is true

To prove, given a biconditional theorem of the form  $H \Leftrightarrow C$ , both  $H \Rightarrow C$  and  $C \Rightarrow H$  needs to be proved.

**Bijection** A function is **bijective** if it is both *injective* and *surjective*. Sometimes also called a *one to one correspondence*.

**Binary Operation** ( $\circ$ ) is a rule defined on a set  $\Omega$  that assigns the objects  $a, b \in \Omega$  to an object  $c$ .

**Boolean Algebra** is a poset  $B$  that satisfies the following:

- $\forall x, y \in B$ , there exists a *supremum*,  $x \vee y$ .

- $\forall x, y \in B$ , there exists a *infimum*,  $x \wedge y$ .
- $\wedge$  distributes over  $\vee$  such that  $\forall x, y, z \in B, x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ .
- $B$  contains the least element 0 and the greatest element 1 of  $B$ .
- Each element  $x$  has a *complement*  $\neg x$ , such that  $x \wedge \neg x = 0$  and  $x \vee \neg x = 1$ .

*Note:* By definition, a Boolean Algebra is a lattice (thus also known as Boolean lattice).

**Cartesian Product** If  $S$  and  $T$  are sets, the **cartesian product** of  $S$  and  $T$  is the set  $S \times T$  of ordered pairs  $(s, t)$  with  $s \in S$  and  $t \in T$ . The ordered pair  $(s, t)$  is determined uniquely by the fact that its first coordinate is  $s$  and its second coordinate is  $t$ .

**Claim** is an assertion that is then proved, often used like an informal lemma.

**Closure** A set  $\Omega$  is **closed** under a binary operation  $\circ$  if and only if  $a \circ b \in \Omega$  whenever  $a, b \in \Omega$ .

To prove, let  $a, b$  be arbitrary but fixed elements in  $\Omega$ , compute  $a \circ b$  and show that  $a \circ b \in \Omega$ .

**Commutative/Abelian** A binary operation  $\circ$  is said to be **commutative** on a set  $\Omega$  and is called an *abelian operation* if and only if  $\forall a, b \in \Omega, a \circ b = b \circ a$ .

To prove, let  $a, b$  be arbitrary but fixed elements in  $\Omega$ , compute  $a \circ b$  and  $b \circ a$  and show that  $a \circ b = b \circ a$ .

**Complete Lattice** is a lattice such that any subset of elements have a meet and join. Thus, every **complete** lattice is bounded.

*Note:* Every finite lattice is complete.

**Composite Function (Composition)** If  $f : S \rightarrow T$  and  $g : T \rightarrow U$ , then the **composite function**  $g \circ f : S \rightarrow U$  is defined to be the unique function with domain  $S$  and codomain  $U$  for which  $(g \circ f)(x) = g(f(x))$  for all  $x \in S$ . In category theory, it is necessary that the codomain of  $f$  be the domain of  $g$  in order for  $g \circ f$  to be defined.

**Compound Statement** is combined from simple logical statements that is based on more than one object and the use of logical operators.

**Conditional Statement/Implication** ( $\Rightarrow$ ) Let  $P$  and  $Q$  be statements, then the declarative sentence  $P \Rightarrow Q$  is called a **conditional statement**.

*Note:* In the statement  $P \Rightarrow Q$ ,  $P$  is also called the *antecedent* and  $q$  the *consequent*

**Conjecture** is any mathematical statement that has not yet been proved or disproved. To disprove a **conjecture**, a *counterexample* is required. A *counterexample* to the conjecture  $H \Rightarrow C$  is a specific example where the hypothesis  $H$  is true, but the conclusion  $C$  is false.

*Note:* only a single counterexample is needed to disprove a **conjecture**

**Conjunction** ( $\wedge$ ) is a truth-functional operator that is true if and only if *all* of its operands are true.

**Continuum** A set  $X$  is said to have the **power of the continuum** or is said to have **cardinality  $\mathfrak{c}$**  iff it is equivalent to the unit interval  $[0, 1]$  (note that not all infinite sets are denumerable, e.g. the unit interval  $[0, 1]$  is non-denumerable).

*Note:*  $\mathbb{R}$ , the set of real numbers, has cardinality  $\mathfrak{c}$ . Every interval in  $\mathbb{R}$ , open or closed, has cardinality  $\mathfrak{c}$ . And hence, any interval is equivalent to  $\mathbb{R}$ .

**Continuum Hypothesis:** There does not exist a set  $A$  with the property that  $\aleph_0 < \#(A) < \mathfrak{c}$ .

**Contradiction** is a statement that is always false for all of its states of nature.

**Contrapositive Statement** The **contrapositive** of the statement  $P \Rightarrow Q$  is  $\neg P \Rightarrow Q$ .

*Note:* a statement and its contrapositive are logically equivalent

**Converse Statement** The **converse** of the statement  $P \Rightarrow Q$  is  $Q \Rightarrow P$ .

*Note:* a statement and its converse are not logically equivalent

**Corestriction** If  $f : S \rightarrow T$ ,  $g : S \rightarrow B$  and  $T \subseteq B$ , then  $f$  is the **corestriction** of  $g$  to  $T$  if  $g = i \circ f$ , where  $i$  is the inclusion of  $T$  in  $B$ .

**Corollary** is a theorem that can be stated as a special case of a more general theorem. Also is a result in which the (usually short) proof relies heavily on a given theorem. Often say that "this is a corollary of Theorem A".

**Deductive Reasoning** is the method of reasoning where a conclusion is reached by logical arguments based on a collection of assumptions.

**Diagonal Relation** ( $\Delta_S$ ) A relation from  $S$  to  $S$  for any set  $S$  defined as:

$$\Delta_S = \{(x, x) | x \in S\}$$

**Direct Proof** Prove if  $H$  then  $C$ , that is  $H \Rightarrow C$ :

Forward Direct Approach Assume that the hypothesis  $H$  is true, proceeds forward with a sequence of logical arguments that leads to the conclusion  $C$ .

Proof by Contrapositive State the contrapositive to prove; if  $\neg C$  then  $\neg H$ ,  $\neg C \Rightarrow \neg H$ . Assume the conclusion  $C$  is false (ie:  $\neg C$  is true), proceeds forward using the forward directoy approach that eventually leads to the negation of the hypothesis  $H$  (ie:  $\neg H$  is true).

**Disjunction** ( $\vee$ ) is a truth-functional operator that is true if and only if *one or more* of its operands are true.

**Empty Set** ( $\emptyset$ ) is the set with no elements  $\{\}$ .

**Equivalence Class** If  $R$  is an equivalence relation in  $A$ , then the **equivalence class** of any element  $a \in A$  denoted by  $[a]$ , is the set of elements to which  $a$  is related:

$$[a] = \{x : \langle a, x \rangle \in R\}$$

**Equivalence Relation** A relation  $R$  in a set  $A$  (a subset  $R$  of  $A \times A$ ), is an **equivalence relation** iff it satisfies the following axioms:

*Reflexive:* For every  $a \in A$ ,  $\langle a, a \rangle \in R$

*Symmetric:* If  $\langle a, b \rangle \in R$ , then  $\langle b, a \rangle \in R$

*Transitive:* If  $\langle a, b \rangle \in R$  and  $\langle b, c \rangle \in R$ , then  $\langle a, c \rangle \in R$

**Existence Proof** is used to prove an *Existence Theorem* of the nature:

*There exists an object  $A$  that is an element of the set  $C$  that has property  $P$*

Proof of an existence theorem requires showing that  $\exists A \in C$  that has the property  $P$ , can be as simple as constructing an object  $A$  in  $C$  with property  $P$ .

*Note:* this may require a great deal of creative thinking and mathematical insight to construct/create the object required for the proof. It is not unusual that a mathematical trick or an uncommon approach is required to construct the object.

**Existential Quantification** ( $\exists$ ) is read as *there exists, there is at least one, there is some*.

*Note:* negating an existentially quantified statement is equivalent to the statement with an universal quantifier but with the associated propositional function negated

**Fixed Point** A **fixed point** of a function  $f : S \rightarrow S$  for a set  $S$  is an element  $x \in S$  such that  $f(x) = x$ .

**Function** ( $\rightarrow$ ) A **function**  $f$  is a mathematical entity with the following properties:

1.  $f$  has a **domain** and **codomain**, each of which must be a set.
2. For every element  $x$  of the domain,  $f$  has a **value** at  $x$ , which is an element of the codomain and is denoted  $f(x)$ .
3. The domain, the codomain, and the value  $f(x)$  for each  $x$  in the domain are all determined completely by the function.
4. Conversely, the data consisting of the domain, the codomain, and the value  $f(x)$  for each element  $x$  of the domain completely determine the function  $f$ .

The domain and codomain are often called the **source** and **target** of  $f$ .

*Range:* of  $f : A \rightarrow B$ , denoted by  $f[A]$ , is the set of images:  $f[A] = \{f(a) : a \in A\}$ .

*Equivalence:* Two functions  $f : A \rightarrow B$  and  $g : A \rightarrow B$  are equal, written  $f = g$ , iff  $f(a) = g(a)$  for every  $a \in A$  (i.e. iff they have the same graph).

*Negation:* of  $f = g$  is written  $f \neq g$  and is the statement  $\exists a \in A$  for which  $f(a) \neq g(a)$ .

*Relation:* A subset  $f$  of  $A \times B$  (a relation from  $A$  to  $B$ ) is a function iff for each  $a \in A$  appears as the first coordinate in exactly one ordered pair  $\langle a, b \rangle \in f$ .

*Composition:* Given functions  $f : A \rightarrow B$  and  $g : B \rightarrow C$ , the function  $g \circ f : A \rightarrow C$  (called the **composition** of  $f$  and  $g$ ) maps the element  $a \in A$  into the element  $g(f(a)) \in C$ .

*Inverse:* In general, the inverse relation  $f^{-1}$  of a function  $f \subseteq A \times B$  need not be a function. However, if  $f$  is both *injective* and *surjective*, then  $f^{-1}$  is a function from  $B$  to  $A$  and is the **inverse function**.

$$f^{-1} \circ f = id_A \text{ and } f \circ f^{-1} = id_B$$

**Graph of a Function** is the set of ordered pairs:  $\{(x, f(x)) | x \in S\}$  for a function  $f : S \rightarrow T$ . The graph of a function from  $S$  to  $T$  is a relation from  $S$  to  $T$  that for all  $s \in S$ , there is one and only one  $t \in T$  such that  $(s, t)$  is in the graph, sometimes known as **mapping** from  $s$  to  $t$ .

**Heyting Algebra** is a bounded lattice where  $\vee$  and  $\wedge$  are the join and meet operations and has an implication binary operation  $a \Rightarrow b$  that satisfies the condition  $(x \wedge a) \leq b$  if and only if  $x \leq (a \Rightarrow b)$ .

*Note:* A heyting algebra is *complete* if its lattice structure is complete.

**Homomorphism** is a structure preserving map between two *algebraic structures* of the same type (such as *groups, graphs, rings, vector spaces*)

*Graph Homomorphism:*

For a graph  $\mathcal{G}$ , let  $G_0$  denote the set of nodes and  $G_1$  denote the set of paths/arrows. A *graph homomorphism*  $\phi$  from a graph  $\mathcal{G}$  to a graph  $\mathcal{H}$  denoted  $\phi : \mathcal{G} \rightarrow \mathcal{H}$ , is a pair of functions  $\phi_0 : \mathcal{G}_0 \rightarrow \mathcal{H}_0$  and  $\phi_1 : \mathcal{G}_1 \rightarrow \mathcal{H}_1$  with the property that if  $u : m \rightarrow n$  is an arrow of  $\mathcal{G}$ , then  $\phi_1(u) : \phi_0(m) \rightarrow \phi_0(n)$  in  $\mathcal{H}$ .

**Monoid Homomorphism:**

A *monoid homomorphism* between two monoids  $(M, *)$  and  $(N, \bullet)$  is a function  $f : M \rightarrow N$  such that  $f(x * y) = f(x) \bullet f(y)$  for all  $x, y \in M$  and  $f(e_M) = e_N$ .

**Identity** is a mathematical expression giving the equality of two (often variable) quantities. (Ex: *trigonometric identities, Euler's identity*)

**Identity Function** (*id*) Every set  $S$  has an **identity function**  $id_S : S \rightarrow S$  for which  $id_S(x) = x$  for all  $x \in S$ .

**Image** is the set of values of a function  $f : S \rightarrow T$ ,  $\{t \in T \mid \exists s \in S, f(s) = t\}$ .

**Inclusion Function** If a set  $S$  is a subset of a set  $T$  (denoted by  $S \subseteq T$ ), then there is an **inclusion function**  $i : S \rightarrow T$  for which  $i(x) = x$  for all  $x \in S$ .

*Note:* the functions  $id_S$  and  $i$  are different functions because they have different codomains, even though their value at each element of their (common) domain is the same

**Indexed Set** An **indexed class of sets**  $\mathcal{A}$ , denoted by:

$$\{A_i : i \in I\}, \{A_i\}_{i \in I} \text{ or simply } \{A_i\}$$

assigns a set  $A_i$  to each  $i \in I$  (a function from  $I$  into a class of sets). The set  $I$  is called the *index set*, the sets  $A_i$  are called **indexed sets**, and each  $i \in I$  is called an *index*.

*Sequence:* When the index set  $I$  is the set of positive integers, the indexed class  $\{A_1, A_2, \dots\}$  is called a **sequence** (of sets). We write

$$\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup \dots \text{ and } \bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap \dots$$

for the union and intersection respectively.

*Cartesian Product:* for an indexed class of sets  $\mathcal{A}$  is denoted by:

$$\prod \{A_i : i \in I\} \text{ or } \prod_{i \in I} A_i \text{ or simply } \prod_i A_i$$

is the set of all functions  $p : I \rightarrow \cup_i A_i$  such that  $p(i) = a_i \in A_i$ . We denote such an element of the Cartesian product by  $p = \langle a_i : i \in I \rangle$ . For each  $i_0 \in I$  there exists an  $i_0$ th *projection function*,  $\pi_{i_0}$ , from the product set  $\prod_i A_i$  into the  $i_0$ th *coordinate set*  $A_{i_0}$  defined by:

$$\pi_{i_0}(\langle a_i : i \in I \rangle) = a_{i_0}$$

*Union:* for an indexed class of sets  $\mathcal{A}$  is denoted by:

$$\bigcup \{A_i : i \in I\}, \bigcup_{i \in I} A_i \text{ or } \cup_i A_i$$

*Intersection:* for an indexed class of sets  $\mathcal{A}$  is denoted by:

$$\bigcap \{A_i : i \in I\}, \bigcap_{i \in I} A_i \text{ or } \cap_i A_i$$

**Indirect Proof/Proof by Contradiction** (*reductio ad absurdum*) Prove if  $H$  then  $C$ . Assume the hypothesis  $H$  is true and conclusion  $C$  is false. Proceeds forward with a sequence of logical arguments until a contradiction is formed.

*Note:* proving  $\neg(H \Rightarrow C)$  is always false (a contradiction) is logically equivalent to proving that  $H \Rightarrow C$  is true

**Inductive Reasoning** is the method of reasoning based on making inferences and conclusions from observations to a more general conclusion or future event.

**Infimum** ( $\sqcap$ ) is the *greatest lower bound* of a subset  $T$  of a poset  $S$  denoted as  $\sqcap T$  or  $\inf(T)$ , if such an element exists.

**Injection** Also known as **one to one**, a function  $f : S \rightarrow T$  is **injective** if whenever  $s \neq s'$  in  $S$ , then  $f(s) \neq f(s')$  in  $T$ .

*Note:* Do not confuse the definition of **injective** with the property that if  $s = s'$ , then  $f(s) = f(s')$ . Another way to say that a function is injective is via the contrapositive: if  $f(s) = f(s')$ , then  $s = s'$

**Kleene Closure** (\*) The **Kleene Closure**  $A^*$  of a set  $A$  is the set of lists of finite length of elements of  $A$ . Example,  $(a, b, d, a)$  is an element of  $\{a, b, c, d\}^*$ .

*Note:*  $A^*$  contains the empty list  $()$  and  $\forall a \in A$ , the lists  $(a)$  with length 1.

**Lattice** is a poset in which every pair of elements have a unique supremum and infimum.

*Note:* A lattice  $L$  is *bounded* if it has a greatest element 1 and least element 0 such that for every element  $x \in L$ ,  $0 \leq x \leq 1$ .

*Note:* In any lattice,  $\top$  and  $\perp$  are called *improper elements*. All other elements are called *proper*.

*Note:* If  $f$  and  $g$  are functions from  $D$  to  $D'$  where  $D, D'$  are complete lattices, then  $f \leq g$  if  $f(x) \leq g(x)$  for all  $x \in D$ .

**Least Upper Bound Axiom** If  $A$  is a set of real numbers bounded from above, then  $A$  has a **least upper bound**, i.e.  $\sup(A)$  exists.

*Example:* The set  $\mathbb{Q}$  of rational numbers does not satisfy the Least Upper Bound Axiom. For let

$$A = \{q \in \mathbb{Q} : q > 0, q^2 < 2\}$$

i.e.,  $A$  consists of those rational numbers which are greater than 0 and less than  $\sqrt{2}$ . Now  $A$  is bounded from above, e.g. 5 is an upper bound for  $A$ . But  $A$  does not have a least upper bound, i.e. there exists no rational number  $m$  such that  $m = \sup(A)$ . If included,  $\sqrt{2}$  would be the least upper bound, however  $m$  cannot be  $\sqrt{2}$  since  $\sqrt{2}$  does not belong to  $\mathbb{Q}$ .

**Archimedean Order Axiom:** The set  $\mathbb{N} = \{1, 2, 3, \dots\}$  of positive integers is not bounded from above.

In other words, there exists no real number which is greater than every positive integer. One consequence of this theorem is:

There is a rational number between any two distinct real numbers.

**Lemma** is a minor result whose sole purpose is to help in proving a theorem. Any provable result that is used primarily as a necessary step in the proof of another theorem, a stepping stone on the path to proving a theorem. Very occasionally lemmas can take on a "life of their own" (*Zorn's lemma*, *Urysohn's lemma*, *Burnside's lemma*, *Sperner's lemma*).

**Logical Operators** Let  $P$  and  $Q$  be statements:

- $P \wedge Q$  is called the *conjunction* or *meet* of the statements  $P$  and  $Q$
- $P \vee Q$  is called the *disjunction* or *join* of the statements  $P$  and  $Q$

- $\neg P$  is called the *negation* of the statement  $P$

**Logical Statement/Proposition** is a declarative sentence that is either true or false.

**Logically Equivalent** Two statements  $X$  and  $Y$  are **logically equivalent** when they have identical truth tables.

**Mathematical Definition** is a statement that gives precise meaning to a mathematical concept, word or term. It characterizes the meaning of the word by giving all the properties and only those properties that must be true.

**Mathematical Induction** A special type of direct proof that can often be used with theorems of the nature:

The statement  $P(n)$  holds for every natural number  $n$  (ie: holds for a statement indexed by  $n$  for all  $n \in \mathbb{N}$ ).

Weak Induction: Prove  $\forall n \in \mathbb{N} P(n)$ .

Initial Step (Base Case): show  $P(1)$  is true

Induction Step: if  $P(k)$  is true for an arbitrary but fixed (ABF) value of  $k$  in  $\mathbb{N}$ , then it follows that  $P(k+1)$  is also true

Strong Induction: Same as *Weak Induction* except in the *Induction Step*: instead of assuming only  $P(k)$  is true, assume that  $P(1), \dots, P(k)$  are all true for an ABF value of  $k$  in  $\mathbb{N}$

*Note:* *Weak* and *Strong* inductions are logically equivalent to each other. In general, attempt a proof with weak induction, if a stronger inductive hypothesis is required, use strong induction. It is important that the initial step must lead to the induction step (ie:  $P(1)$  leads to  $P(2)$ ,  $P(1)$  is true leads to  $P(2)$  being true).

**Monoid** is a *semigroup* with an *identity element*.

**Monotone Function** is a function between *ordered sets* that preserves or reverses the given order.

*Example:* A function  $f : D \rightarrow D'$  between lattices  $D$  and  $D'$  is monotonic if  $f(x) \leq f(y)$  whenever  $x \leq y$ .

**Negation** ( $\neg$ ) is an unary logical operator that inverts the true values of a proposition. If  $P$  is a proposition,  $\neg P$  is false when  $P$  is true, true when  $P$  is false.

**Nested Interval Property** Let  $I_1 = [a_1, b_1]$ ,  $I_2 = [a_2, b_2]$ ,  $\dots$  be a sequence of **nested closed (bounded) intervals**, i.e.  $I_1 \supseteq I_2 \supseteq \dots$ . Then there exists at least one point common to every interval, i.e.

$$\bigcap_{i=1}^{\infty} I_i \neq \emptyset$$

It is necessary that the intervals in the theorem be closed and bounded.

*Examples:*

- Let  $A_1, A_2, \dots$  be the following sequence of open-closed intervals:

$$A_1 = (0, 1], A_2 = (0, \frac{1}{2}], \dots, A_k = (0, \frac{1}{k}], \dots$$

Now the sequence of intervals is nested ( $A_1 \supseteq A_2 \supseteq \dots$ ) but the intersection of the intervals is empty, i.e.,

$$A_1 \cap A_2 \cap \dots \cap A_k \cap \dots = \emptyset$$



– Let  $A_1, A_2, \dots$  be the following sequence of closed infinite intervals:

$$A_1 = [1, \infty), A_2 = [2, \infty), \dots, A_k = [k, \infty), \dots$$

Now  $A_1 \supseteq A_2 \supseteq \dots$  but there exists no point common to every interval, i.e.,

$$A_1 \cap A_2 \cap \dots \cap A_k \cap \dots = \emptyset$$

**Order** Define an **order** relation in  $\mathbb{R}$ , using the concept of positiveness.

The real number  $a$  is *less than* the real number  $b$ , written  $a < b$ , if the difference  $b - a$  is positive.

Further notation include:

- $b > a$  means  $a < b$
- $a \leq b$  means  $a < b$  or  $a = b$
- $b \geq a$  means  $a \leq b$

From the axioms  $(P_1)$  and  $(P_2)$  defined in positive numbers. Let  $a, b, c \in \mathbb{R}$ , then:

- either  $a < b$ ,  $a = b$  or  $b < a$
- if  $a < b$  and  $b < c$ , then  $a < c$
- if  $a < b$ , then  $a + c < b + c$
- if  $a < b$  and  $c$  is positive, then  $ac < bc$
- if  $a < b$  and  $c$  is negative, then  $ac > bc$

*Note:* The set  $\mathbb{R}$  of real numbers is totally ordered by the relation  $a \leq b$ .

**Ordered  $n$ -Tuple** is a sequence  $(a_1, \dots, a_n)$  determined uniquely by the fact that for  $i = 1, \dots, n$ , the  $i$ th coordinate of  $(a_1, \dots, a_n)$ , is  $a_i$ . Then the cartesian product  $S_1 \times S_2 \times \dots \times S_n$  is the set of all  $n$ -tuples  $(a_1, \dots, a_n)$  with  $a_i \in S_i$  for  $i = 1, \dots, n$

**Ordered Set** is a set  $X$  with a relation  $R$  defining an **order** on its elements, denoted by  $\preceq$ . If  $a \preceq b$ , then we say that  $a$  *precedes* or *is smaller* than  $b$  and that  $b$  *follows*, *dominates* or *is larger* than  $a$ . We write  $a \prec b$  if  $a \preceq b$  but  $a \neq b$ .

*First and Last Elements:* An element  $a_0 \in X$  is a **first** or **smallest** element of  $X$  iff  $a_0 \preceq x$  for all  $x \in X$ . Similarly, an element  $b_0 \in X$  is a **last** or **largest** element of  $X$  iff  $x \preceq b_0$  for all  $x \in X$ .

*Maximal and Minimal Elements:* An element  $a_0 \in X$  is **maximal** iff  $a_0 \preceq x$  implies  $x = a_0$ , i.e. if no element follows  $a_0$  except itself. Similarly, an element  $b_0 \in X$  is **minimal** iff  $x \preceq b_0$  implies  $x = b_0$ , i.e. if no element precedes  $b_0$  except itself.

**Paradox** is a statement that can be shown, using a given set of axioms and definitions, to be both true and false. A paradox is often used to show the inconsistencies in a flawed theory (*Russell's paradox*), used informally to describe a surprising or counterintuitive result that follows from a given set of rules (*Banach-Tarski paradox*, *Alabama paradox*, *Gabriel's horn*).

**Partial Function** A **partial function**  $f : S \rightarrow T$  is a function where  $f$  is only defined on  $S_0 \subseteq S$ .

**Partial Order** ( $\preceq$ ) is a binary relation that is *reflexive*, *antisymmetric* and *transitive* (ie: a partial order is an antisymmetric preorder).

**Partially Ordered Set/Poset** is a *preordered set*  $(X, \preceq)$  where  $\preceq$  is *antisymmetric*, (ie: a set  $X$  with a partial order).

*Inverse Order:* If a relation  $R$  in a set  $A$  defines a partial order, then the inverse relation  $R^{-1}$  is also a partial order; it is called the **inverse order**.

*Upper and Lower Bounds:* Let  $A \subseteq X$ . An element  $m \in X$  is a **lower bound** of  $A$  iff  $m \preceq x$  for all  $x \in A$ , i.e. if  $m$  precedes every element in  $A$ . If some lower bound of  $A$  follows every other lower bound of  $A$ , then it is called the infimum or *greatest lower bound*. Similarly, an element  $M \in X$  is an **upper bound** of  $A$  iff  $x \preceq M$  for all  $x \in A$ , i.e. if  $M$  follows every element in  $A$ . If some upper bound of  $A$  precedes every other upper bound of  $A$ , then it is called the supremum or *least upper bound*.

*Note:*  $A$  is said to be *bounded above* if it has an upper bound, and *bounded below* if it has a lower bound. If  $A$  has both an upper and lower bound, then it is said to be *bounded*.

**Partially Ordered Subset** Let  $A \subseteq X$ , where  $X$  is a poset. Then the order in  $X$  induces an order in  $A$ : If  $a, b \in A$ , then  $a \preceq b$  as elements in  $A$  iff  $a \preceq b$  as elements in  $X$ . More precisely, if  $R$  is a partial order in  $X$ , then the relation  $R_A = R \cap (A \times A)$ , called the *restriction* of  $R$  to  $A$ , is a partial order in  $A$ . The ordered set  $(A, R_A)$  is called a **(partially ordered) subset** of the ordered set  $(X, R)$ .

*Note:* Some subsets of a poset may be totally ordered.

**Partition** A class  $\mathcal{A}$  of non-empty subsets of  $A$  is called a **partition** of  $A$  iff (1) each  $a \in A$  belongs to some member of  $\mathcal{A}$  and (2) the members of  $\mathcal{A}$  are pair-wise disjoint.

*Note:* There is a one to one correspondence between the set of equivalence classes (or the quotient set  $A/R$ ) and a partition of  $A$ .

**Path** In a graph  $\mathcal{G}$ , a **path** from a node  $x$  to a node  $y$  of length  $k$  is a sequence  $(f_1, f_2, \dots, f_k)$  of directed edges for which:

- $source(f_k) = x$
- $target(f_i) = source(f_{i-1})$  for  $i = 2, \dots, k$
- $target(f_1) = y$

The empty path is denoted as  $()$ .

**Pointed Set** is a set  $S$  equipped with a distinguished element  $s \in S$ . This element is called a *pointed object*.

**Positive Numbers** are defined by the following axioms:

( $P_1$ ) If  $a \in \mathbb{R}$ , then exactly one of the following is true:  $a$  is positive;  $a = 0$ ;  $-a$  is positive.

( $P_2$ ) If  $a, b \in \mathbb{R}$ , then their sum  $a + b$  and their product  $a \bullet b$  are also positive.

It follows that  $a$  is positive iff  $-a$  is negative.

*Example:* The product  $a \bullet b$  of a positive number  $a$  and a negative number  $b$  is negative.

For if  $b$  is negative then, by ( $P_1$ ),  $-b$  is positive and so, by ( $P_2$ ), the product  $a \bullet (-b)$  is also positive. But  $a \bullet (-b) = -(a \bullet b)$ . Thus  $-(a \bullet b)$  is positive and so, by ( $P_1$ ),  $a \bullet b$  is negative.

**Power Set ( $\mathcal{P}$ )** The **power set**  $\mathcal{P}(S)$  of any set  $S$  is the set of all subsets of  $S$ , including the empty set.

**Preimage/Inverse Image ( $^{-1}$ )** For a set function  $f : X \rightarrow Y$ , the **preimage**  $f^{-1} : \mathcal{P}(B) \rightarrow \mathcal{P}(A)$  of a set  $B \subseteq Y$  is a subset of  $X$  defined by:

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

**Preorder** is a binary relation that is both *reflexive* and *transitive*.

**Preordered Set** is a set  $S$  with a preorder  $\alpha$  defined on its elements, denoted as  $(S, \alpha)$ .

**Projection (Coordinate) Function** If  $S$  and  $T$  are sets, their cartesian product  $S \times T$  is equipped with two **coordinate** or **projection functions**  $proj_1 : S \times T \rightarrow S$  and  $proj_2 : S \times T \rightarrow T$ . The coordinate functions are surjective if  $S$  and  $T$  are both nonempty.

**Proof** A proof of a mathematical result is a sequence of rigorous mathematical arguments that are presented in a clear and concise fashion. Convincingly demonstrates the truth of a given result.

*Remarks:*

- no method of proof begins with the assumption that the conclusion is true
- no method of proof begins with the assumption that the hypothesis is false
- if a conjecture cannot be proved, it may be false. To disprove, provide a counterexample

**Proof by Cases** is a proof where the paths of the logical arguments leads to a statement involving an either/or statement such as conditions  $S_1$  or condition  $S_2$ , it is often useful to consider separate proofs for each of the cases. If the same arguments are used for proofs of two or more cases, then the cases should be combined into a single case. In the situation of similar cases, a *without loss of generality* (WLOG) statement may be used to shorten the proof of a similar case.

*Note:* there may be more than 2 cases

**Proper Subset ( $\subset$ )** In the case that  $A \subseteq B$  but  $A \neq B$ , we say that  $A$  is a **proper subset** of  $B$  and write  $A \subset B$ .

**Propositional Function** is a declarative sentence  $P(x)$  involving a variable  $x$  that takes on values in a set  $\Delta$  is said to be a **propositional function** iff  $P(x)$  has a well-defined truth value for each value of  $x$  in  $\Delta$ . The set  $\Delta$  is called the *domain* of the propositional function  $P(x)$ .

**Quotient Set** is the collection of equivalence classes of  $A$  with the equivalence relation  $R$ , denoted by  $A/R$ . Also called the *quotient* of  $A$  by  $R$ .

$$A/R = \{[a] : a \in A\}$$

**Real Numbers ( $\mathbb{R}$ )** when viewed as a set  $\mathbb{R}$ , can be characterized by the statement that  $\mathbb{R}$  is a *complete, Archimedean ordered field*.

*Subsets of Real Numbers:*

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

where

$$\text{Natural Numbers } \mathbb{N} = \{1, 2, 3, \dots\}$$

$$\text{Integers } \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

$$\text{Rational Numbers } \mathbb{Q} = \{x \in \mathbb{R} : x = \frac{p}{q}; p, q \in \mathbb{Z}, q \neq 0\}$$

The is also the set of *irrational numbers* is defined by  $\mathbb{I} = \mathbb{Q}^c$  where  $\mathbb{Q}^c$  is the complement of  $\mathbb{Q}$  in  $\mathbb{R}$ .

**Reflexive** is a binary relation  $\alpha$  over a set  $S$  where  $\forall s \in S, s\alpha s$ .

**Relation** A relation  $\alpha$  from a set  $S$  to a set  $T$  is a subset of  $S \times T$ . Any such subset is a relation from  $S$  to  $T$ . Extreme examples of relations are the  $\emptyset$  and the set  $S \times T$ .

*Domain and Range:* The *domain* of a relation  $R$  from  $A$  to  $B$  is the set of first coordinates of the pairs in  $R$  and its *range* is the set of second coordinates. i.e., domain of  $R = \{a : \langle a, b \rangle \in R\}$ , range of  $R = \{b : \langle a, b \rangle \in R\}$ .

*Inverse:* The *inverse* of  $R$ , denoted by  $R^{-1}$ , is the relation from  $B$  to  $A$  defined by domain of  $R = \{a : \langle a, b \rangle \in R\}$ , range of  $R = \{b : \langle a, b \rangle \in R\}$ .

*Composition:* Let  $U$  be a relation from  $A$  to  $B$  and let  $V$  be a relation from  $B$  to  $C$  ( $U \subseteq A \times B$  and  $V \subseteq B \times C$ ), the **composition** of  $U$  and  $V$  is denoted  $V \circ U$ . Which consists of all ordered pairs  $\langle a, c \rangle \in A \times C$  such that for some  $b \in B$ :

$$\langle a, b \rangle \in U \text{ and } \langle b, c \rangle \in V$$

**Relative Complement** of a set  $B$  with respect to a set  $A$  or simply, the *difference* of  $A$  and  $B$ , denoted by  $A \setminus B$ , is the set of elements which belong to  $A$  but not in  $B$ .

$$A \setminus B = \{x : x \in A, x \notin B\}$$

**Restriction** If  $g : S \rightarrow T$ ,  $f : A \rightarrow T$  and  $A \subseteq S$ , then  $f$  is the **restriction** of  $g$  to  $A$  (also denoted  $g|A$ ) if  $f = g \circ i$  where  $i : A \rightarrow S$  is the inclusion function of  $A$  in  $S$ . Equivalently,  $f = g|A = g \cap (A \times Y)$ .

*Note:*  $g$  is also called an *extension* of  $f$ .

**Schroeder-Bernstein Theorem** We write  $A \preceq B$  if  $A$  is equivalent to a subset of  $B$ ,

$$A \preceq B \text{ iff } \exists B^* \subseteq B \text{ s.t. } A \sim B^*$$

The **Schroeder-Berstein Theorem** states that  $A \preceq B$  and  $B \preceq A$ , then  $A \sim B$ . This can also be restated as:

$$\text{Let } X \supseteq Y \supseteq X_1 \text{ and let } X \sim X_1, \text{ then } X \sim Y$$

In terms of cardinality, this can also be stated as: If  $\#(A) \leq \#(B)$  and  $\#(B) \leq \#(A)$ , then  $\#(A) = \#(B)$ .

*Note:* We also write  $A \prec B$  if  $A \preceq B$  but  $A \not\sim B$ , if  $A$  is not equivalent to  $B$ .

*Example:* Since  $\mathbb{N} \subset \mathbb{R}$ ,  $\mathbb{N} \preceq \mathbb{R}$ . In fact,  $\mathbb{R}$  is not denumerable, i.e.  $\mathbb{R} \not\sim \mathbb{N}$ , and thus  $\mathbb{N} \prec \mathbb{R}$ .

*Law of Trichotomy:* Given any pair of sets  $A$  and  $B$ , either  $A \prec B$ ,  $A \sim B$  or  $B \prec A$ .

*Note:* If  $A \prec B$  then we say that  $A$  has cardinality less than  $B$  or  $B$  has cardinality greater than  $A$ .

$$\#(A) < \#(B) \text{ iff } A \prec B$$

**Semidirect Product** The **semidirect product** of monoids  $M$  and  $T$  with the action  $\alpha : M \times T \rightarrow T$  is the monoid with the underlying set  $T \times M$  where  $\alpha$  is defined as:

- $\forall m \in M, \alpha(m, 1_T) = 1_T$
- $\forall m \in M, \forall t, t' \in T, \alpha(m, tt') = \alpha(m, t)\alpha(m, t')$
- $\forall t \in T, \alpha(1_M, t) = t$
- $\forall m, m' \in M, \forall t \in T, \alpha(mm', t) = \alpha(m, \alpha(m', t))$

and multiplication of the semidirect product is:

$$(t, m)(t', m') = (t\alpha(m, t'), mm')$$

for all  $t, t' \in T$  and  $m, m' \in M$ .

*Note:* The action  $\alpha$  can be thought of a monoid homomorphism  $\phi : M \rightarrow \mathbf{End}(T)$  where  $\mathbf{End}(T)$  is the monoid of endomorphisms of  $T$ .

**Semigroup** is a set  $S$  together with an associative and closed binary operation,  $m : S \times S \rightarrow S$ .

**Semilattice** A poset with a join for any nonempty finite subset is a **join-semilattice/upper semilattice**. Dually, a poset with a meet for any nonempty finite subset is a meet-semilattice/lower semilattice.

**Set** is a mathematical entity that is distinct from, but completely determined by, its elements (if any). For every entity  $x$  and set  $S$ , the statement  $x \in S$ , read " $x$  is an element of  $S$ ", is a sentence that is either true or false.

*Note:* When members of a set  $A$  are sets themselves,  $A$  may be called a *class*, *collection*, or *family*.

*Set Equality:*

- Two sets  $A$  and  $B$  are equal, written  $A = B$ , if they consist of the same elements. Note that sets do not depend on the way they are displayed, a set remains the same if its elements are repeated or rearranged.
- Two sets  $A$  and  $B$  are equal if and only if  $A \subseteq B$  and  $B \subseteq A$ .

Note that this is different from the concept of set equivalence.

**Set Cardinality (#)** If  $A$  is equivalent to  $B$  ( $A \sim B$ ), then we say that  $A$  and  $B$  have the same **cardinal number** or **cardinality**. We write  $\#(A)$  for "the cardinal number (or cardinality) of  $A$ ".

$$\#(A) = \#(B) \text{ iff } A \sim B$$

*Note:* The cardinal numbers of  $\mathbb{N}$  and the interval  $[0, 1]$  are:

$$\aleph_0 (\text{read: aleph-null}) = \#(\mathbb{N}), \mathbf{c} = \#([0, 1])$$

A set  $X$  is said to have cardinality  $\aleph_0$  iff it is equivalent to  $\mathbb{N}$ . And  $0 < 1 < 2 < \dots < \aleph_0 < \mathbf{c}$ .

*Finite:* A set is **finite** iff it is empty or equivalent to  $\{1, 2, \dots, n\}$  for some  $n \in \mathbb{N}$ . Otherwise it is said to be **infinite**.

*Denumerable:* A set is called **denumerable** if it has cardinality  $\aleph_0$ . Note that every infinite set contains a denumerable subset.

*Countable:* A set is called **countable** iff it is finite or denumerable. Note that Every subset of a countable set is countable.

*Note:* A set which is neither finite nor denumerable is said to be *non-denumerable* or *non-countable*.

*Cantor's Theorem:* The power set  $\mathcal{P}(A)$  of any set  $A$  has cardinality greater than  $A$ .

**Set Equivalence ( $\sim$ )** A set  $A$  is called **equivalent** to a set  $B$ , written  $A \sim B$ , if there exists a function  $f : A \rightarrow B$  which is both *injective* and *surjective*. The function  $f$  is then said to define a *one-to-one correspondence* between the sets  $A$  and  $B$ . By this definition, two finite sets are equivalent iff they contain the same number of elements.

*Note:* For finite sets, equivalence corresponds to the usual meaning of two sets containing the same number of elements.

*Note:* An infinite set can be equivalent to a proper subset of itself, this property is true of infinite sets in general.

**Set Intersection** ( $\cap$ ) Let  $\mathcal{A}$  be any class of subsets of the universal set  $U$ . The **intersection** of the sets in  $\mathcal{A}$ , denoted by  $\cap\{A : A \in \mathcal{A}\}$ , is the set of elements which belong to every set in  $\mathcal{A}$ :

$$\cap\{A : A \in \mathcal{A}\} = \{x : x \in U, \forall A \in \mathcal{A}, x \in A\}$$

*Note:*  $\cap\{A : A \in \emptyset\} = U$  and  $\cap\{A_i : i \in \emptyset\} = U$ . Ref: [4]

**Set Union** ( $\cup$ ) Let  $\mathcal{A}$  be any class of subsets of the universal set  $U$ . The **union** of the sets in  $\mathcal{A}$ , denoted by  $\cup\{A : A \in \mathcal{A}\}$ , is the set of elements which belong to at least one set in  $\mathcal{A}$ :

$$\cup\{A : A \in \mathcal{A}\} = \{x : x \in U, \exists A \in \mathcal{A} \text{ s.t. } x \in A\}$$

*Note:*  $\cup\{A : A \in \emptyset\} = \emptyset$  and  $\cup\{A_i : i \in \emptyset\} = \emptyset$ . Ref: [4]

**Singleton Set** (**1**) is any set with exactly one element,  $\{a\}$ , where  $a$  is the only element. **Space** is used to refer to a non-empty set which possesses some type of mathematical structure, e.g. *vector space*, *metric space* or *topological space*. In such a situation, the elements in a space are called *points*.

**Subset** ( $\subseteq$ ) A set  $A$  is a **subset** of a set  $B$ , or equivalently,  $B$  is a **superset** of  $A$ , written  $A \subseteq B$  or  $B \supseteq A$  iff each element in  $A$  also belongs to  $B$ ; that is, if  $x \in A$  implies  $x \in B$ .

*Note:* The negation of  $A \subseteq B$  is written  $A \not\subseteq B$  or  $B \not\supseteq A$  and states that there is an  $x \in A$  such that  $x \notin B$ .

*Note:* The words *subclass*, *subcollection* and *subfamily* are sometimes used to indicate subsets where their elements are sets themselves.

**Supremum** ( $\sqcup$ ) is the *least upper bound* of a subset  $T$  of a poset  $(S, \preceq)$ . That is, for a subset  $T \subseteq S$ , a **supremum** is an element  $v \in S$  such that:

- $\forall t \in T, t \preceq v$
- If  $w \in S$  has the property that  $t \preceq w$  for every  $t \in T$ , then  $v \preceq w$

*Note:* The supremum of  $T$  is denoted as  $\sqcup T$  or  $\sup(T)$ .

**Surjection** Also known as **onto**, a function  $f : S \rightarrow T$  is **surjective** if its image is  $T$ . For instance, the identity function on any set is **surjective**, but no other inclusion function is.

**Tautology** is a statement that is always true for all of its states of nature.

**Theorem** is any mathematical statement that can be shown to be true using accepted logical and mathematical arguments.

**Totally (or Linearly) Ordered Set** is a partially ordered set  $A$  if for every  $a, b \in A$ , either  $a \preceq b$  or  $b \preceq a$ .

*Example:*  $\mathbb{R}$  with the natural order defined by  $x \leq y$  is a totally ordered set.

**Transitive** is a binary relation *alpha* over a set  $S$  if whenever an element  $a$  is related to an element  $b$ , and  $b$  is related to an element  $c$ , then  $a$  is also related to  $c$ . Thus,  $\forall a, b, c \in S, (a\alpha b \wedge b\alpha c) \Rightarrow a\alpha c$ .

**Uniqueness Proof** is used to prove an *Uniqueness Theorem* of the nature:

*Object  $A$  that is an element of the set  $C$  is the only (unique) object having a property  $P$*

An uniqueness proof shows that one and only one object has the special property  $P$ . Uniqueness theorems in general can be proved via proof by contradiction: show object  $A \in C$  has property  $P$ , assume  $A$  is not unique (ie: another object  $B \in C$  exists with property  $P$  where  $B \neq A$ ), then using logical arguments, show that  $B = A$ .

**Universal Quantification** ( $\forall$ ) is read as *for every, for each, for all*.

*Note:* negating an universally quantified statement is equivalent to the statement with an existential quantifier but with the associated propositional function negated

**Universal Set** ( $U$ ) In any application of the theory of sets, all sets under investigation are subsets of a fixed set. We call this set the **universal set** or **universe of discourse** and denote it as  $U$ . Thus for any set  $A$ ,  $A \subseteq U$ .

**Variables in Propositional Functions** is any term in a propositional function whose value is not explicitly stated, implied or understood and whose value is needed in order to determine the truth or falsity of the proposition. The values of a variable is called the *domain* of the propositional function and is denoted by  $\Delta$ .

**Zorn's Lemma** Let  $X$  be a non-empty poset in which every totally ordered subset has an upper bound. Then  $X$  contains at least one maximal element.

*Remark:* This is equivalent to the classical *Axiom of Choice* and the *Well-ordering Principle*.

## References

- [1] Charles Wells Michael Barr. *Category Theory for Computing Science*. Reprints in Theory and Applications of Categories #22. 2013.
- [2] Stoy J.E. *Denotational semantics: The Scott-Strachey approach to programming language theory*. MIT, 1977.
- [3] Lipschutz S. *Theory and applications of general topology*. Schaum's outlines. 1965.
- [4] Ittay Weiss ([https://math.stackexchange.com/users/30953/ittay weiss](https://math.stackexchange.com/users/30953/ittay_weiss)). Empty intersection and empty union. Mathematics Stack Exchange. URL:<https://math.stackexchange.com/q/370201> (version: 2020-05-24).