Topic 1: Sets and Logic[1]

The Language of Sets

A **set** is a collection of distinct objects. Usually, we use the braces, $\{\}$, to represent the sets. The objects inside the braces are called **elements** of the set.

For example, here are some sets:

- $A = \{\text{peaches, kiwis, berries}\}$
- $S = \{0, 1, 2\}$
- $\emptyset = \{\}$
- $\mathbb{N} = \{1,\ 2,\ ...\}$

A set that contains no elements at all, as in the third example, is called an **empty set** and is mathematically denoted as $\emptyset$.

Usually, we use upper capital letters to denote sets (e.g., S), and use lowercase letters to denote elements (e.g., x). To denote membership or inclusion in a set, we use the symbol $\in$. We denote "x is an element of the set S" with $x \in S$. For example, peaches $\in A$. We can also denote "x is *not* an element of the set S" with $x \notin S$. For example, bananas $\notin A$.

Example 1

True or false:

- $0 \in \{0, 1, 2\}$
- $0 = \{0\}$
- $\emptyset \in \emptyset$
- $\emptyset \in S$
- $S \in S$
- $S \in \mathbb{N}$

[1] Instructors: Camilo Abbate and Sofia Olguin. This note was prepared for the 2025 UCSB Math Camp for Ph.D. students in economics. It incorporates materials from previous instructors, including Shu-Chen Tsao, ChienHsun Lin, and Sarah Robinson.

In set theory, a set can be defined in two ways:

- **Extensionally** (by enumeration), by listing all of its elements.
- **Intensionally** (by description), by describing a property that defines its members.

On the previous examples, we used extensional definitions, listing each element within the sets. However, we can also define a set intensionally, using a condition to describe its elements, as illustrated below:

$$\{x \mid x \text{ has property } P.\}$$

means the collection of all elements that have the property P.

Sometimes you may also see notations like

$$\{x \in A \mid x \text{ has property } P.\},$$

which is equivalent to

$$\{x \mid x \in A \;\text{ and }\; x \text{ has property } P.\}.$$

Here we list some set notations that are commonly used.

$\mathbb{N}$	Set of natural numbers $\{1, 2, 3, \dots\}$. Some textbooks also include 0.
$\mathbb{Z}$	Set of integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{R}$	Set of real numbers (whole number line)
$\mathbb{R}^+$ or $\mathbb{R}_+$	Set of positive real numbers. Some textbooks define it as non-negative.
(a, b)	The open interval between real numbers a and b ($\{x \in \mathbb{R} \mid a < x < b\}$)
$[a, b]$	The closed interval between real numbers a and b ($\{x \in \mathbb{R} \mid a \leq x \leq b\}$)

Example 2

Rewrite the follow sets as listing all the elements:

- $\{x \in \mathbb{Z} | \; x \text{ is an even number.}\}$
- $\{x \geq 0 \mid x \text{ is an even number.}\}$
- $\{p \in \mathbb{Z} \mid p > 10 \text{ and } p < 2\}$

Definition 1 (Subsets)

For any two sets A and B, we say A is a **subset** of B if every element of A is also an element of B. We denote it as $A \subset B$ (or $A \subseteq B$).
If $A \subset B$ and $B \subset A$, we say A and B are **equal sets** ($A = B$).
If $A \subset B$ but $B \not\subset A$, we say A is a **proper subset** of B ($A \subsetneq B$).

Two sets are **equal sets** if they contain exactly the same elements. We write $A = B$ whenever $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$.[2] By definition, $A \subset B$ implies that every element of A also belongs to B; that is, $x \in A \Rightarrow x \in B$. Therefore, two sets are equal if and only if each is a subset of the other: $A = B$ if and only if $A \subset B$ and $B \subset A$.

Example 3

True or false:

- $\{0, 2\} \subset \{x \geq 0 \mid x \text{ is an even number.}\}$
- $\{0, 2\} \subset \{x > 0 \mid x \text{ is an even number.}\}$
- $\{0, 2\} \subset \{0, 2\}$
- $\emptyset \subset \{0, 2\}$
- $\emptyset \subset \emptyset$

Power Set

For any given set S, we can list all of its possible subsets. The collection of subsets of a set is called **the power set**.

Definition 2 (Power Set)

For any set S, **the power set** of the set S, denoted as $\mathcal{P}(S)$, is defined as the following:

$$\mathcal{P}(S) = \{A \mid A \subset S\}.$$

For example, the power set of $S = \{a, b, c\}$ is

$$\mathcal{P}(S) = \{\{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

The empty set, $\emptyset$, is in the power set of any set as it is a subset of any set, including itself.

[2] The symbol $\Rightarrow$ denotes logical implication. A formal definition will be provided later in these notes.

Cardinality of a Set

You can also count the number of elements in a set. The **cardinality** of the set A, denoted with $|A|$, is the number of elements in the set A.

If the number of elements in a set is finite, we call this set a **finite** set. If the number of the elements in a set is infinite, we call this set a **infinite** set.

However, there could be several levels of infinity. First, consider the set of all natural numbers, $\mathbb{N}$. It has infinitely many elements in it. Then we consider another set which has all non-negative integers, $\mathbb{Z}^+$. It seems that $\mathbb{Z}^+$ has more elements than $\mathbb{N}$. However, you can actually *count* the elements in $\mathbb{Z}^+$,

$$\begin{array}{ccccccc} \mathbb{Z}^+ = \{ & 0, & 1, & 2, & 3, & \ldots \} \\ & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \end{array}$$

you can find a *one-to-one correspondence (bijection)* between the natural numbers and non-negative integers.[3] Therefore we say $\mathbb{Z}^+$ has the same cardinality as $\mathbb{N}$ ($|\mathbb{Z}^+| = |\mathbb{N}|$), or $\mathbb{Z}^+$ is **countable** (or **countably infinite**).

You can even show that $\mathbb{Z}$ is also countable by indexing the elements in $\mathbb{Z}$ in the following alternating way:

$$\begin{array}{cccccccc} \mathbb{Z} = \{ \ldots & \text{-2}, & \text{-1}, & 0, & 1, & 2, & \ldots \} \\ & \mathbf{5} & \mathbf{3} & \mathbf{1} & \mathbf{2} & \mathbf{4} & \end{array}$$

Although not rigorously proven here, all subsets of $\mathbb{Z}$ and $\mathbb{Q}$ are also countable. However, $\mathbb{R}$ is uncountable.[4]

We can also consider the cardinality of the power set. If S is a finite set with n elements, then $\mathcal{P}(S)$ contains 2^n elements. That is, $|\mathcal{P}(S)| = 2^{|S|}$. In the previous section's example, we defined $S = \{a, b, c\}$, then $\mathcal{P}(S)$ has $2^3 = 8$ elements.

[3] We will review bijection in a few days.

[4] For the proof of the uncountability of $\mathbb{R}$, check *Cantor's diagonal argument* for reference.

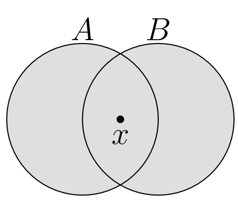
Set Operations

Just like that you can add or subtract numbers, you can also perform operations on sets.

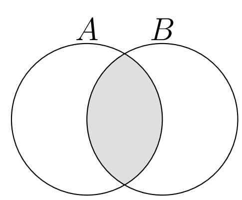
Definition 3 (Set operations)

- Union: $A \cup B \coloneqq \{x \mid x \in A \textit{ or } x \in B\}$.
- Intersection: $A \cap B \coloneqq \{x \mid x \in A \textit{ and } x \in B\}$.
- Difference: $A \setminus B$ or $A - B \coloneqq \{x \mid x \in A \textit{ and } x \notin B\}$.

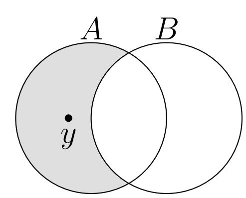
The figures below demonstrate these operations. These figures are called **Venn diagrams**. We use Venn diagrams to illustrate the relation between the sets. For example, in the left diagram in the first row, x is in the circles of both sets A and B, which represents that $x \in A$ and $x \in B$. Similarly, y is in the circle of set A but not in set B, which represents $y \in A \setminus B$ (right diagram). Finally, the intersection is represented in the central diagram. Note that when $A \cap B = \emptyset$, we say A and B are **disjoint sets** (as shown in the left figure in the second row).



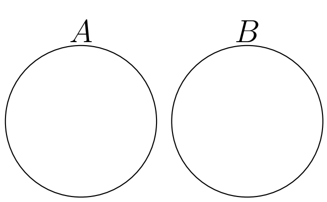
Union: $A \cup B$



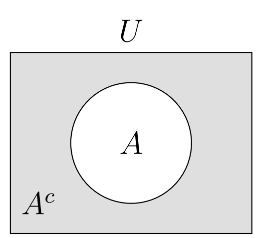
Intersection: $A \cap B$



Difference: $A \setminus B$



Disjoint Sets



A and A^c

We can define a **universal set** U that contains all the elements of interest. Then the **complement** of the set A, A^C or $\overline{A}$, is defined as

$$A^C = U \setminus A = \{x \mid x \in U, x \notin A\}.$$

We can take unions or intersections of more than two sets. We usually use the following notation.

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n, \qquad \bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n.$$

The definition for the union or the intersection of multiple sets is similar to the two-set case. For example,

$$A \cup B \cup C = \{x \mid x \in A \text{ or } x \in B \text{ or } x \in C\}.$$

We can also take unions or intersections of infinitely many sets.

Proposition 1 presents some useful facts that you may try to verify by yourself.

Proposition 1 (Distributive and associative property of set operations)

For any sets A, B, and C,

1. $A \setminus B = A \cap B^C$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (Distributive property)
3. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distributive property)
4. $A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C)$ (Associative property)
5. $A \cap B \cap C = (A \cap B) \cap C = A \cap (B \cap C)$ (Associative property)

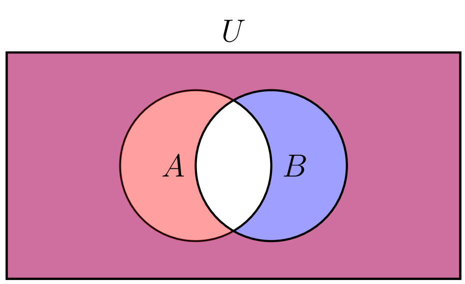
Proposition 2 (De Morgan's Law)

For any two sets A and B,

(1) $(A \cup B)^C = A^C \cap B^C$.

(2) $(A \cap B)^C = A^C \cup B^C$.

We will now launch our first proof in this course. The first step of showing something, is to understand *what is going to be shown*. In the first part, we will show that the sets $(A \cup B)^C$ and $A^C \cap B^C$ are equal to each other. You may want to draw a Venn diagram to "prove" the proposition. Indeed, if you draw it, you will likely find that the proposition looks correct.



De Morgan's Law

However, drawing a Venn diagram is NOT a legit proof, especially if you just draw one. The proposition requires the condition *for any* two sets A and B. Drawing only one Venn diagram shows the one and only one very specific case that is represented with the graph. Nevertheless, graphing is still a very nice way to give yourself a quick glance at what the proposition is talking about and sometimes a hint about how you should proceed the proof.

How can we rigorously show the two sets are **equal**? You can try going back to the definition above: for any two sets A and B, $A = B$ if $A \subset B$ and $B \subset A$. Then we can establish the goal: to show that the two sets are subsets of each other.

Proof. We firstly show $(A \cup B)^C \subset A^C \cap B^C$. Pick $x \in (A \cup B)^C$. By definition, $x \notin A \cup B$. From this, we can know that $x \notin A$ and $x \notin B$, because if $x \in A$ or $x \in B$, x must belong to $A \cup B$ by definition. Hence, $x \in A^C$ and $x \in B^C$. By definition, it implies $x \in A^C \cap B^C$. Note that it is always true for any x that we pick. Therefore, $(A \cup B)^C \subset A^C \cap B^C$.

Then we show $A^C \cap B^C \subset (A \cup B)^C$. Pick $x \in A^C \cap B^C$. By definition, $x \in A^C$ and $x \in B^C$, which implies $x \notin A$ and $x \notin B$. Hence, $x \notin A \cup B$, so $x \in (A \cup B)^C$. Note that it is always true for any x that we pick. Therefore, $A^C \cap B^C \subset (A \cup B)^C$.

Since $(A \cup B)^C$ and $A^C \cap B^C$ are subsets of each other, $(A \cup B)^C = A^C \cap B^C$. ■

The above is the style of proof that you might read in textbooks, which is sometimes not the easiest to understand. You may also try the style of proof presented below.

Proof. WTS (want to show): $(A \cup B)^C \subset A^C \cap B^C$.

$$
\begin{aligned}
& x \in (A \cup B)^C && \text{(take any } x \in (A \cup B)^C\text{)} \\
\Rightarrow & x \notin A \cup B && \text{(definition of complements)} \\
\Rightarrow & x \notin A \text{ and } x \notin B && \text{(by contradiction and definition of the union)} \\
& && \text{(if } x \in A \text{ or } x \in B,\ x \in A \cup B.\text{)} \\
\Rightarrow & x \in A^C \text{ and } x \in B^C && \text{(definition of complements)} \\
\Rightarrow & x \in A^C \cap B^C && \text{(definition of intersection)} \\
\Rightarrow & (A \cup B)^C \subset A^C \cap B^C && \text{(definition of subsets).}
\end{aligned}
$$

■

The other part of the proof is omitted. One thing to note is that: the former statement should always imply the latter statement when you write arrows. We will elaborate more when we talk about logic and proofs.

Partitions of a Set

Just like cutting a cake, you can cut a set into a collection of several subsets. This collection of subsets is called a **partition** of the set.

Definition 4 (Partition)

A collection of non-empty sets $\mathcal{P}$ is called a **partition** of a set S if it satisfies the following conditions:

(1) For every set $A \in \mathcal{P}$, $A \subset S$
(2) If $A \neq B$ and $A, B \in \mathcal{P}$, then $A \cap B = \emptyset$.
(3) $\bigcup_{A \in \mathcal{P}} A = S$.

Partitions are useful in probability theory. For example, how can we calculate the probability of the event "getting two Heads when tossing two coins"? We can split the set of all possible events into partitions where each part has the same probability to happen, and *count* what's the proportion that the "two-Heads" event happens in the partition. This is known as the **frequentist probability**.[5]

Example 4

Consider $S = \{1, 2, 3, 4\}$.

- Possible partition 1: $\mathcal{P}_1 = \{\{1\}, \{2\}, \{3\}, \{4\}\}$
- Possible partition 2: $\mathcal{P}_2 = \{\{1, 3\}, \{2, 4\}\}$
- Possible partition 3: $\mathcal{P}_3 = \{\{1, 2, 4\}, \{3\}\}$

Note that the partitions of the set S, in Example 4, are all subsets of the power set of S.

[5] You can also give a *measure* to the elements in a partition. We can define a **probability space** with respect to a partition (sigma algebra) and some valid probability measure.

Cartesian Product

The elements in a set are *unordered*. That is, the order in which we list elements does not change the essence of the set. However, there are situations when we need to consider mathematical objects with a specific order.

For example, let $x \in X = \{\text{labor, capital}\}$, $y \in Y = \{\text{output A, output B}\}$, and x produces y. We can have sentences like "labor produces output A" or "capital produces output B," but not "output A produces labor".

In the preceding example, the tuple (x, y) is an **ordered** pair; the order of the elements has meaning. The Cartesian product is used to describe the collection of such ordered pairs.

Definition 5 (Cartesian product)

Let X and Y be two sets. The **Cartesian product** of the two sets, $X \times Y$ (read as "X cross Y"), is defined as

$$X \times Y = \{(x, y) |\ x \in X \text{ and } y \in Y\}.$$

If $X = Y = \mathbb{R}$, then $X \times Y = \mathbb{R}^2$, the 2-dimensional Cartesian coordinate system.

In general, $X \times Y$ does not equal $Y \times X$, as seen in the above case. (Preference) relations are one of the most important applications of Cartesian products in economics.

Example 5

Let X be the set of the goods that can be chosen. For any $x \in X$ and $y \in X$, we write $x \succsim y$ if x is preferred to y. We can use the tuple (x, y) to express $x \succsim y$. The set of all such tuples can be expressed with the Cartesian product $\succsim \subset X \times X$.

a) If $X = \{a, b, c\}$, find $X \times X$.

We know Moona has the following preference:

$$a \succsim_M b,\ a \succsim_M c,\ b \succsim_M c,$$

then we can write $(a, b) \in \succsim_M$, $(a, c) \in \succsim_M$, and $(b, c) \in \succsim_M$.

Suppose Nina has the following preference:

$$a \succsim_N a,\ a \succsim_N b,\ a \succsim_N c,\ b \succsim_N b, b \succsim_N c, c \succsim_N c.$$

b) Find the relation $\succsim_N$. Is $\succsim_N = \succsim_M$?

Ordered Sets

Definition 6 (Total Order)

Let S be a set. A relation $\leq$ defined on S is a **total order** if:
(1) Reflexivity: $x \leq x$ for any $x \in S$.
(2) Antisymmetry: if $x \leq y$ and $y \leq x$, then x and y are the same.
(3) Transitivity: if $x \leq y$ and $y \leq z$, then $x \leq z$.
(4) Completeness: Either $x \leq y$ or $y \leq$ x.

Definition 7 (Ordered Set)

A set S is a **(total) ordered set** if there is a total order defined on S.

The notation "less than or equal to" ($\leq$) is commonly used to represent the ordering relation in an ordered set. It naturally captures the idea of one element being less than or the same as another, which aligns with the intuitive understanding of order.

Example 6

Convince yourself that the set of real numbers $\mathbb{R}$ is a total ordered set. The set of rational numbers Q is also a total ordered set.

The game of Rock-Paper-Scissors does not form an ordered set. Which property in the definition of total order is violated?

Definition 8 (Boundedness)

Suppose S is an ordered set and $E \subset S$.

If there exists $\beta \in S$ such that $x \leq \beta$ for every $x \in E$, we say that E is **bounded above**. We call β an **upper bound** of E.

If there exists $\alpha \in S$ such that $x \geq \alpha$ for every $x \in E$, we say that E is **bounded below**. We call α a **lower bound** of E.

Definition 9 (Supremum: Least Upper Bound)

Suppose S is an ordered set, and $E \subset S$. Suppose E is bounded above.

If there exists $\underline{\beta} \in S$ with the following properties:
(1) $\underline{\beta}$ is an upper bound of E, and
(2) for every upper bound of E, β, $\underline{\beta} \leq \beta$

Then $\underline{\beta}$ is called the **least upper bound** of E, or the **supremum** of E, and we write $\underline{\beta} = \sup E$.

Definition 10 (Infimum: Greatest Lower Bound)

Suppose S is an ordered set, and $E \subset S$. Suppose E is bounded above.

If there exists $\bar{\alpha} \in S$ with the following properties:
(1) $\bar{\alpha}$ is a lower bound of E, and
(2) for every lower bound of E, α, $\alpha \leq \bar{\alpha}$

Then $\bar{\alpha}$ is called the **greatest lower bound** of E, or the **infimum** of E, and we write $\bar{\alpha} = \inf E$.

Notice that we only require $\sup E$ and $\inf E$ to be in S, so $\sup E$ and $\inf E$ may or may not be in E.

Example 7

Let $E \subset \mathbb{R}$ consist of all numbers $\frac{1}{n}$, where $n = 1, 2, 3, \ldots$.

Convince yourself:
(1) 1000 is a upper bound of E.
(2) -1000 is a lower bound of E.
(3) 1 is the least upper bound of E, which is in E.
(4) 0 is the greatest lower bound of E, which is not in E.

Axioms

An **axiom** is a statement that is "taken to be true." It serves as a starting point for further reasoning and arguments. Reasoning based on axioms is fundamental in microeconomic theory.

For example, suppose we want to prove that "I strictly prefer A to B" and "I strictly prefer B to A" cannot hold at the same time. We have the intuition that they cannot hold at the same time, but how can we formally prove this intuition? In microeconomic theory, we first propose a set of axioms that arguably "make sense." Then, we show that when these axioms are true, these two statements cannot hold at the same time. Writing proofs based on a given set of axioms is essential in Econ 210A.[6]

Logic

Logic is the field of study that determines the truthfulness and relations between statements. In order to analyze the statements, we need to brake the statements into the atomic units: propositions. Here we start with the simplest case, that a proposition P can either be **true** or **false**. We say "P has the truth value of T" if P is true, and we say "P has the truth value of F" if P is false.

We can use a **truth table** to express the truth values of the proposition. For propositions P and Q, we can have truth values as follows.

P	Q
T	T
T	F
F	T
F	F

Since P and Q can either be true or false, there are in total four combinations of the truth states.

[6] In other fields of mathematics, the most common sets of axioms include the Peano axioms and the Zermelo–Fraenkel Choice (ZFC) axioms.

Logical Operators

Here we list some logical operators.

1. $\neg$ – Negation: $\neg P$, read as "not P."
2. $\wedge$ – Conjunction: $P \wedge Q$, read as "P and Q."
3. $\vee$ – Disjunction: $P \vee Q$, read as "P or Q."
4. $\Rightarrow$ – Implication: $P \Rightarrow Q$, read as "P implies Q" or "if P, then Q."
5. $\Leftrightarrow$ – Equivalence: $P \Leftrightarrow Q$, read as "P and Q are logically equivalent."

The result of applying a logical operator to propositions is itself a proposition, so we can determine its truth value. Below are the truth tables for propositions involving these operators.

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

You may find that the truth table somewhat reflects how we read these operators. For example, $\neg P$ is true only when P is false; $\neg P$ is false only when P is true. Similarly, $P \wedge Q$ is true when and only when both P and Q are true; if either P or Q is false, $P \wedge Q$ is false.

Note that $P \vee Q$ may contradict our daily use of **or**.[7] We usually mean either P or Q are true, but not both. In computer science, this is called **exclusive or**, **strong or**, or **xor**.

Example 8

For any statements P, Q, and R, show that each group of statements below has the same truth table.

(1) $\neg(\neg P)$ v.s. P (Double Negation)

(2) $\neg(P \wedge Q)$ v.s. $\neg P \vee \neg Q$ (De Morgan's Law)

(3) $\neg(P \vee Q)$ v.s. $\neg P \wedge \neg Q$ (De Morgan's Law)

(4) $P \Rightarrow Q$ v.s. $\neg P \vee Q$ v.s. $\neg(P \wedge \neg Q)$ (Implication)

(5) $P \Rightarrow Q$ v.s. $\neg Q \Rightarrow \neg P$ (Contrapositive)

(6) $(P \wedge Q) \Rightarrow R$ v.s. $P \Rightarrow (Q \Rightarrow R)$ (Exportation)

(7) $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ v.s. $P \Leftrightarrow Q$

(8) $(P \Leftrightarrow Q) \wedge (Q \Leftrightarrow R)$ v.s. $P \Leftrightarrow R$ (Transitivity of equivalence)

[7] "Would you like coffee or tea?" "Yes. "

Implication

Implication is the center of mathematical arguments. We usually use the implications to derive the conclusions we demand from the assumption that we know. In a statement $P \Rightarrow Q$, P is usually called the **premise** or the **assumption**, and Q is called the **conclusion**.

We can translate the following sentences into $P \Rightarrow Q$.

If P, then Q.
Q if P.
P only if Q.
P implies Q.
P is sufficient for Q.
Q is necessary for P.

First, note that "if" and "only if" represent the complete opposite directions of the implication. Also notice the last two sentences above: when $P \Rightarrow Q$ is true, we call P the **sufficient condition** of Q, and Q the **necessary condition** of P.

You might find that the truth table for the implication is not very intuitive. Note that $P \Rightarrow Q$ is only false when P is true and Q is false. Statements such as "If a square has three sides, then the moon is made of cheese" or "Isla Vista is the largest city in the U.S. implies that the GDP of the U.S. in 2023 is decreased by 5%" both are true statements. Indeed, *any false premise implies any conclusion* is a true statement.

The key here is that we are finding whether the occurrence of P implies Q. P and Q are the evidences that may reveal this implication. If P is not true, we cannot prove that the implication $P \Rightarrow Q$ is false. In that case, as the implication is not proven false, it is true.

Example 9

Suppose P, Q, and R are statements. Use the truth table to show that the following statements are always true.

(1) $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ (*modus ponens*)
(2) $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$ (*modus tollens*)
(3) $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ (*syllogism*)

If you explain *Modus ponens* in words, it says "when you know P is true, and you know if P then Q, Q is hence true". In fact, this is how an argument works. On the other hand, *syllogism* provides the "chain" of arguments. These two rules form the basis of direct proof.

In Example 8, we also find rules related to implications. Specifically, (5) shows that $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$ share the same truth table. We call $\neg Q \Rightarrow \neg P$ the **contrapositive** of $P \Rightarrow Q$, and $Q \Rightarrow P$ its **converse**. While a statement is logically equivalent to its contrapositive, which is important in mathematical arguments, it is not, in general, equivalent to its converse.

Logical Equivalence

When the statements P and Q always have the same truth value, we say P and Q are **logically equivalent**, denoted as $P \Leftrightarrow Q$ or $P \equiv Q$. The pairs of statements we saw in Example 8 are logically equivalent.

From (7) in Example 8, we see that when both $P \Rightarrow Q$ and $Q \Rightarrow P$ hold, P and Q are logically equivalent. To indicate this, we use "P if and only if Q", often abbreviated as "iff".

The following sentences can be translated into $P \Leftrightarrow Q$.

P if and only if (iff) Q.
P is equivalent to Q.
P characterizes Q.
P is a sufficient and necessary condition for Q.
P is defined as Q.

Compound Propositions, Tautologies, and Contradictions

A **compound proposition** is a proposition formed by combining statements using logical operators. Depending on how it is formulated, a compound proposition may always be true or always false.

A compound statement that is always true is called a **tautology**, whereas one that is always false is called a **contradiction**.

For example, for any proposition P,

$$P \vee (\neg P)$$

is always true, while

$$P \wedge (\neg P)$$

is always false.

The statements in Example 9 are all tautologies. Do not confuse tautology with logical equivalence.

Open Sentences and Quantifiers

Some statements cannot be determined true or false until they are completed. For example,

$$P(x): \; x \geq 2.$$

We would not know whether this statement is true or false until we know which x we are talking about. When $x = 2$, it is true; when $x = 1$, it is false. This type of statement $P(x)$ is called an **open sentence**.

To determine the truth value of an open sentence, we need to specify the elements to be inserted into the sentence.[8]

Definition 11 (Some Quantifiers)

- $\forall$ – Universal quantifier
  "$\forall x \in X, \; P(x)$" is true if *$P(x)$ is true for every $x \in X$.*
- $\exists$ – Existential quantifier
  "$\exists x \in X$ such that $P(x)$" is true if *there exists an $x \in X$ such that $P(x)$ is true.*
- $\exists!$ – Uniqueness existential quantifier
  "$\exists! x \in X$ such that $P(x)$" is true if *there exists* ***one and only one*** *$x \in X$ such that $P(x)$ is true.*

Sometimes an open sentence can be an tautology. That is, no matter which x is inserted, it is always true. For example,

$$P(x): \; x^2 \geq 0$$

is always true for any $x \in \mathbb{R}$ (although not necessarily true for some $x \in \mathbb{C}$).

[8] If X is not specified, we consider all x in the universe U.

Here is a useful property when dealing with the quantifiers. Carefully read this statement.

Proposition 3

If $P(x)$ is an open sentence with variable x, and X is a set, then

(1) $\neg(\forall x \in X,\ P(x)) \Leftrightarrow \exists x \in X$ such that $\neg P(x)$.

(2) $\neg(\exists x \in X$ such that $P(x)) \Leftrightarrow \forall x \in X,\ \neg P(x)$.

In general, the statements switching quantifiers, that is,

$$\forall x,\ \exists y \text{ such that } P(x,y) \quad \text{and} \quad \exists y \text{ such that } \forall x,\ P(x,y)$$

are not equivalent.

We can verify this by an example: for any integer x, there is some integer y that is larger than x. That is,

$$\forall x \in \mathbb{Z},\ \exists y \in \mathbb{Z} \text{ such that } y > x \quad \text{and} \quad \exists y \in \mathbb{Z} \text{ such that } \forall x \in \mathbb{Z},\ y > x$$

are not equivalent, where the former is true while the latter is not.

You may feel that the statements with quantifier has a lot of similarities to the set language. Indeed, we can rewrite the statements with sets. For example, consider the statement $\forall x$, $P(x) \Rightarrow Q(x)$. Let

$$P = \{x \mid P(x) \text{ is true}\},\ Q = \{x \mid Q(x) \text{ is true}\}.$$

By definition, P is a subset of Q if and only if every element in P belongs to Q. Symbolically,

$$P \subset Q \ \Leftrightarrow\ (\forall x, x \in P \Rightarrow x \in Q) \ \Leftrightarrow\ (\forall x, P(x) \text{ is true} \Rightarrow Q(x) \text{ is true}).$$

When properly defined, the logical statements can all be represented by the set language.

References

Chiang, A. and Wainwright, K. (2005). *Fundamental Methods of Mathematical Economics*. McGraw-Hill international edition. McGraw-Hill Education.

Smith, D., Eggen, M., and Andre, R. (2010). *A Transition to Advanced Mathematics*. Cengage Learning.

Topic 2: Proof Strategies [1]

Elements in a Mathematical Proof

A proof is the process of establishing the validity of a statement in a way that is consistent with the rules of logic. To prove a statement means to show that its conclusion follows from a set of premises, using a sequence of logical steps.

The initial statements or premises we *assume* to be true are called **assumptions**, typically introduced with phrases like "*Suppose...*" or "*Assume...*". Any statement implied from these assumptions is only guaranteed to be true if the assumptions themselves are true.

The **conclusion** is the goal of the proof and the statement we aim to establish. Therefore, proving a statement involves demonstrating that its conclusion logically follows from its assumptions, given the truth of these assumptions. We may also rely on **definitions**, which are sets of logically equivalent statements that can be used interchangeably.

We will cover several proof methods: direct proof, proof by contrapositive, proof by contradiction, and mathematical induction. We will also review equivalence proofs and proofs with quantifiers.

Direct Proof

Direct Proof is a way of proving statements that directly connects premises with implications. Let us consider the following example.

Example 1

We define an integer $x \in \mathbb{Z}$ is **even** if there exists an integer k such that $x = 2k$, and an integer $x \in \mathbb{Z}$ is **odd** if there exists an integer k such that $x = 2k + 1$. Show that if n is an odd integer, then $3n + 7$ is an even integer.

[1] Instructors: Camilo Abbate and Sofia Olguin. This note was prepared for the 2025 UCSB Math Camp for Ph.D. students in economics. It incorporates materials from previous instructors, including Shu-Chen Tsao, ChienHsun Lin, and Sarah Robinson.

Proof. When we analyze the proof, we need to find the premises and conclusions. The starting point is that "n is an odd integer", and the goal is "$3n+7$ is an even integer", which can be written as

$$n \text{ is an odd integer} \;\Rightarrow\; 3n+7 \text{ is an even integer.}$$

We also have definitions of odd and even integers that we can replace original statements with math expressions:

$$\exists k \in \mathbb{Z} \text{ such that } n = 2k+1 \;\Rightarrow\; \exists h \in \mathbb{Z} \text{ such that } 3n+7 = 2h.$$

Note that we use different letters k and h as the place holders as we do not know whether the two integers are the same.

Finally, we establish the connection between statements.

$$\begin{aligned}
&\exists k \in \mathbb{Z} \text{ such that } n = 2k+1 \\
\Rightarrow &\exists k \in \mathbb{Z} \text{ such that } 3n = 3(2k+1) = 2(3k)+3 \\
\Rightarrow &\exists k \in \mathbb{Z} \text{ such that } 3n+7 = 2(3k)+3+7 = 2(3k)+2\times 5 = 2(3k+5)
\end{aligned}$$

Let $h = 3k+5$. Note that $h \in \mathbb{Z}$, and $3n+7 = 2h$. Therefore, by definition, we can conclude that $3n+7$ is an even integer. ■

Proof by contrapositive

Proof by contrapositive exploits the fact that $P \Rightarrow Q$ and its contrapositive, $\neg Q \Rightarrow \neg P$, are logically equivalent. Instead of starting with P and then implying Q, you can start with $\neg Q$ and derive $\neg P$. Once you can establish $\neg Q \Rightarrow \neg P$, by logical equivalence, you have $P \Rightarrow Q$.

Let us prove the statement in Example 1 again using the proof by contrapositive approach.

Proof. Firstly, write down the statement to be proved.

$$3n+7 \text{ is not an even integer} \;\Rightarrow\; n \text{ is not an odd integer.}$$

Rewrite the statement as the math expression.

$$\neg(\exists h \text{ such that } 3n+7 = 2h) \;\Rightarrow\; \neg(\exists k \text{ such that } n = 2k+1).$$

Be very careful here that we have NOT shown the property that if an integer is not an even number, then it is an odd number, and vice versa. Although it sounds very right (and it is indeed right), we can still not use this in our argument until it is proven true. We are only given the definition of an odd integer and and even integer.

We can have a detour to show the property that allows us to exchange oddity and evenness, but let's keep working with the contrapositives. For the previous statement, equivalently,

$$\forall h \in \mathbb{Z},\ 3n + 7 \neq 2h \ \Rightarrow\ \forall k \in \mathbb{Z},\ n \neq 2k + 1.$$

Then we establish the connection between statements.

$$\begin{aligned} &\forall h \in \mathbb{Z},\ 3n + 7 \neq 2h \\ \Rightarrow &\forall h \in \mathbb{Z},\ 3n \neq 2h - 7 \\ \Rightarrow &\forall h \in \mathbb{Z},\ n \neq \frac{2h - 7}{3} \end{aligned}$$

As the statement is true for every $h \in \mathbb{Z}$, it is true for every $k \in \mathbb{Z}$ that $h = 3k + 5$. Hence,

$$\forall k \in \mathbb{Z},\ n \neq \frac{2(3k + 5) - 7}{3} = \frac{6k + 3}{3} = 2k + 1.$$

Therefore, we showed the conclusion of the contrapositive, which implies that the original statement is correct. ■

It may seem very unwise to prove by contrapositive in this case. However, depending on the situation, proving oppositely can be easier than a direct proof. For example, prove by contrapositive will definitely be easier for this statement:

$$3n + 7 \text{ is not an even integer } \Rightarrow\ n \text{ is not an odd integer.}$$

Most of the time, it requires practice to see which is the easier way to prove.

Proof by contradiction

Proof by contradiction (or *reductio ad absurdum*) is also a useful proving technique, especially for proofs that do not have clear implication forms as $P(x) \Rightarrow Q(x)$.

We start by **assuming** that the statement R we are proving is *false*. (We usually begin with the phrase "*Assume, to the contrary, R is false.*") Then we show that this assumption leads to some statements that contradict what we know to be true, resulting in a logical contradiction. Proof by contradiction is essentially showing $\neg R \Rightarrow (P \wedge \neg P)$. As $(P \wedge \neg P)$ is a contradiction, the whole statement can only be true if $\neg R$ is false, which implies that the statement we want to show R is true.

Proof by contradiction is useful to show the negative-sounding statements. See the following example.

Example 2

Prove that there is no smallest positive real number.

Proof. Assume, to the contrary, that there exists a smallest positive real number. Call this real number r. Then, we try to derive some statements that contradict to something that we know to be true.

Let $s = \frac{r}{2}$. Note that $s \in \mathbb{R}$ and $0 < s < r$. Since we indeed find a positive real number smaller than r, r is not the smallest positive real number, which leads to a contradiction. ∎

In the prove above, we assume the negation of the statement we are proving is true. We can easily see that

$$\neg R : \text{there is some } r \text{ that is the smallest positive real number.}$$

It immediately implies

$$S : s = \frac{r}{2} \text{ is not smaller than } r \text{ because } s \neq r.$$

But we also show that

$$\neg S : s = \frac{r}{2} \text{ is smaller than } r.$$

Therefore, we have shown that

$$\neg R \Rightarrow (\neg S \wedge S).$$

where $\neg S \wedge S$ forms a contradiction, and it is reached because we assume $\neg R$ is true.

Therefore, $\neg R$ must be false. In other words, R is true.

Equivalence Proof (Proving $P \Leftrightarrow Q$)

$P \Leftrightarrow Q$ and $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ are logically equivalent. Therefore, to show that any two statements are logically equivalent, you can just **show the two statements imply each other**.

Example 3

Suppose A, B are non-empty sets. Show that $A = B$ if and only if the elements in A and B are identical.

For this statement, you have two directions to prove: **sufficiency** (identical $\Rightarrow A = B$) and **necessity** ($A = B \Rightarrow$ identical). Be very careful that when you are proving one direction, do not take the assumptions or premises you use for the other direction.

Proof. We firstly show sufficiency using a direct proof. Since the elements in the two sets are identical, it is immediate that for every element in A, it must in B, and *vice versa*. By the definition of subsets, this implies $A \subset B$ and $B \subset A$. Consequently, by the definition of equal sets, we have $A = B$.

We then show necessity using a proof by contradiction. Assume the opposite that A and B are not identical. Without loss of generality, assume there exists $x \in A$ such that $x \notin B$. Then, by the definition of subsets. $A \not\subset B$. Lastly, by the definition of equal sets, $A \neq B$ and hence leads to a contradiction. ■

In addition to proving $P \Leftrightarrow Q$, we can also prove a sequence of equivalent statements, such as $P \Leftrightarrow Q \Leftrightarrow R$. You can of course show the equivalence of any two pairs of equivalence, and use the transitivity of equivalence to prove the statement. Nonetheless, you can also prove the statement by showing

$$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \wedge (R \Rightarrow P).$$

In words, you show a full implication circle of all statements.

Why does this work out? Note that implication is transitive, that is,

$$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \;\Rightarrow\; (P \Rightarrow R).$$

Hence, with $R \Rightarrow P$, you can then show the equivalence $P \Leftrightarrow R$. Similarly, whenever there is a circle, you can show the equivalence between any two statements on the circle.

Example 4

Suppose A and B are sets. Show the following statements are equivalent.

1. $A \subset B$.
2. $A \cup B = B$.
3. $A \cap B = A$.

Proof with Quantifiers

There are three logical quantifiers: universal quantifier ("for all"), existential quantifier ("there exists"), and uniqueness existential quantifier ("there exists unique"). Here are the proof strategies for each.

(1) **"For all" statements** $\forall x$, $P(x)$
To show a "for all" statement, you have two approaches.
  (a) Direct proof: Pick any x, and show that $P(x)$ is true. Then claim that "since x is arbitrarily picked, the statement is true for any x." Be *very careful* that you are really arbitrarily picking x without any implicit conditions.
  (b) Proof by contradiction: Assume that there exists x such that $P(x)$ is false. Then show that this leads to a contradiction.

(2) **"There exists" statements** $\exists x$ s.t. $P(x)$.
There is nothing fancy–just try to find some x that satisfies $P(x)$.

(3) **"There exists unique" statements** $\exists! x$ s.th. $P(x)$.
Now you not only need to check that there exists some x makes $P(x)$ true, but you also need to make sure that this x you find is the one and only one x qualified. Here are the steps for uniqueness proofs.
  (i) Find one x, and show that $P(x)$ is true.
  (ii) Assume there exists another $y \neq x$ such that $P(y)$ is true.
  (iii) Show that this leads to a contradiction.

Example 5

Show that there exists a unique x such that $(x-3)^2 = 0$.

Proof. Firstly, it is easy to see that $x = 3$ satisfies the requirement. Then assume that there exists $y \neq 3$ such that $(y-3)^2 = 0$. As $y \neq 3$, either $y > 3$ or $y < 3$.

Consider the first case: $y > 3$. Then $y - 3 > 0$, so $(y-3)^2 > 0$, which contradicts $(y-3)^2 = 0$. Next, consider the second case: $y < 3$. Then $y - 3 < 0$, so $(y-3)^2 > 0$, which contradicts $(y-3)^2 = 0$. Both cases of $y > 3$ or $y < 3$ will lead to contradiction. So, when $y \neq 3$, $(y-3)^2 = 0$ cannot be true. It proves the uniqueness. ■

Next, we come back to the proposition we mentioned earlier.

Proposition 1

$\emptyset$ is a subset of any set S.

This proposition looks very strange to prove directly. Recall the definition of $A \subset S$ is "$\forall x \in A,\ x \in A \Rightarrow\ x \in S$." Nonetheless, there is nothing in an empty set! Although it is possible to show the statement directly (as we will show below), it may seem more intuitive to prove by contradiction.

Proof. We prove the proposition using two methods.

(1) Direct proof
Note that $\emptyset \subset S$ if and only if $\forall x \in \emptyset$, $x \in \emptyset \Rightarrow x \in S$. Since $x \in \emptyset$ is always false, the whole statement is always true by the truth table of the implication operator ($\Rightarrow$). This is true for any chosen S. Therefore $\emptyset \subset S$ for any set S.

(2) Proof by contradiction
Assume the opposite: $\exists x \in \emptyset$ such that $x \in \emptyset$ and $x \notin S$. However, as there can be no element in the empty set. Therefore, $x \in \emptyset$ and $x \notin S$ cannot be true, and we arrive at a contradiction. Therefore, the original statement is true. ■

Sometimes it may be easier to combine different styles of proofs.

Mathematical Induction

Consider the following statement from high school mathematics:

$$\forall n \in \mathbb{N},\ 1 + 2 + \cdots + n \equiv \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

How do you check this statement is true?

Recall that for this "for all" statement, we can use a direct proof or a proof by contradiction. Notice that the direct proof alone does not work because we need to check *all* n and make sure this statement is true, but there are infinitely many n, so we cannot check all of them.

For this type of proof, going over any natural numbers, we can use the **mathematical induction**.[2]

Theorem 1: The Principle of Mathematical Induction

For each positive integer n, let $P(n)$ be a statement.

If
(1) $P(1)$ is true, and
(2) For every positive integer k, $P(k)$ implies $P(k+1)$,
then $P(n)$ is true for every positive integer n.

Proof. We can prove it by contradiction.

Assume the principle of mathematical induction is not true. In other words, assume (1) $P(1)$ is true and (2) For every positive integer k, $P(k)$ implies $P(k+1)$ are both true, but there exist some $x \in \mathbb{N}$ such that $P(x)$ is false.

Let x_s be the smallest integer such that $P(x_s)$ is false. When $x_s = 1$, it contradicts to the assumption that $P(1)$ is true. When $x_s > 1$, the statement $P(x_s - 1) \Rightarrow P(x_s)$ will be false. Since the assumption leads to contradictions, there must be no $x \in \mathbb{N}$ such that $P(x)$ is false. ■

[2] In fact, the principle of mathematical induction requires a set of axioms on natural numbers. Refer to the Peano axioms if you are interested.

Example 6

Show that for every $n \in \mathbb{N}$,

$$1 + 2 + \cdots + n \equiv \sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Proof. To apply mathematical induction, we need to check two conditions:

(1) $P(1)$ is true. It easy to see that $1 = \frac{1(1+1)}{2}$.

(2) For every positive integer k, $P(k)$ implies $P(k+1)$. We need to check the following statement: for any $k \in \mathbb{N}$, if $\sum_{k'=1}^{k} k' = \frac{k(k+1)}{2}$, then $\sum_{k'=1}^{k+1} k' = \frac{(k+1)(k+2)}{2}$.

Note that $\sum_{k'=1}^{k} k' = \frac{k(k+1)}{2}$. Hence

$$\begin{aligned}
&\sum_{k'=1}^{k+1} k' \\
=&\sum_{k'=1}^{k} k' + (k+1) && \text{(by definition of summation)} \\
=&\frac{k(k+1)}{2} + (k+1) && \text{(by the premise in (2))} \\
=&\frac{k(k+1)}{2} + \frac{2(k+1)}{2} && \text{(by arithmetic)} \\
=&\frac{(k+1)(k+2)}{2}.
\end{aligned}$$

Since conditions (1) and (2) are true, by mathematical induction, the statement is true. ■

Mathematical induction is very useful when dealing with statement about all natural numbers. However, mathematical induction can *only* be used to prove whether a statement holds for all natural numbers. If you want to apply mathematical induction, make sure you can write the statement as stated in the Principle of Mathematical Induction.

References

Smith, D., Eggen, M., and Andre, R. (2010). *A Transition to Advanced Mathematics.* Cengage Learning.