Sets, Proofs, and Logic

Alex Houtz*

August 16, 2023

Sets

We start math camp with set theory, as set theory underlies much of the logic and proofs we use.

A **set** is simply a collection of distinct objects. Each object in a set is called an **element** of the set.

Example 1. Take the set of outcomes from flipping a coin twice. Call this set A. Then we can describe A as:

$$A = \{HH, HT, TH, TT\}$$

HH would be considered an element, a, of set A. We would write this as $HH \in A$. Now suppose that $B = \{HH, TT\}$. Note that all of the elements of B, b, are also elements of A. In this case, we say that B is a **subset** of A, written as $B \subseteq A$. More formally, we can write the definition of subset as an implication:

$$B \subseteq A \Leftrightarrow \{b \in B \Rightarrow b \in A\}$$

Sets can also be equal. If set A is equal to set B, then every element in A is in B *and* every element in B is in A. Essentially, $A \subseteq B$ and $B \subseteq A$.

The **null** or empty set, $\emptyset$, is a set containing no elements. By convention, the null set is a subset of every set. The **universal** set is a set containing all elements possible.

*Math Camp Instructor | University of Notre Dame

Consider the coin flipping example again. In this case, the universal set is set A, as A contains every element possible.

Now, consider combining all of the elements in two generic sets A and B that are subsets of universal set X. We call this a **union** of sets, formally defined as:

$$A \cup B = \{x \in X : x \in A \text{ or } x \in B\}$$

In words, the set A union B is the set containing an element that is in either A or B. Note that an element could be in both A and B. If we wanted a set containing only the elements that were in both A and B, we would want A **intersect** B, defined as:

$$A \cap B = \{x \in X : x \in A \text{ and } x \in B\}$$

Figure 1 visually depicts a union and an intersection of sets.

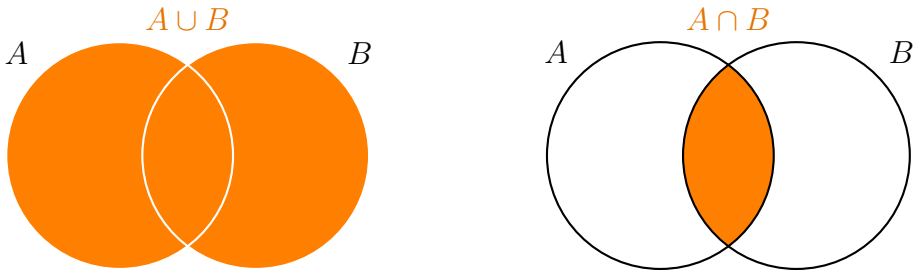

Figure 1: The left panel displays A union B. The right panel displays A intersect B.

Further, suppose we have a set A that is a subset of universal set X. The **complement** of A, denoted as A^c, is the set of $x \in X$ that are not in A. Formally:

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

Example 2. Suppose $X = \{HH, TT, HT, TH\}$ and $A = \{HH, TT\}$. Then $A^c = \{HT, TH\}$.

Now let $B = \{HT\}$. If we take the intersection of A and B, we get the null set. In this case, we call A and B **disjoint**.

Consider figure 2 below. Note that sets A_1 through A_4 are mutually disjoint. Note also that their union is X. We call sets A_1 through A_4 a **partition** of X. We are now ready to define our first theorem:

Theorem 1 (Partitioning Theorem)**.** *If* $\{B_1, B_2, \dots\}$ *is a partition of* X*, then for any set* A*:*

$$A = \bigcup_{i=1}^{\infty} A \cap B_i$$

and the sets $(A \cap B_i)$ *are mutually disjoint.*

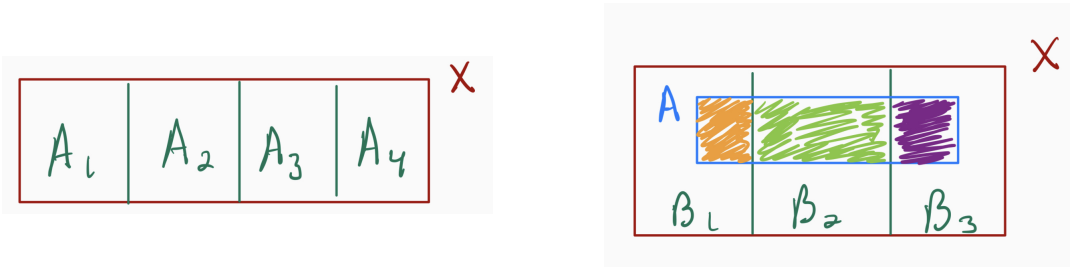

Figure 2: The left panel displays a partition of X. The right panel displays the partitioning theorem.

Besides "adding" sets, we can "multiply" sets using a **Cartesian product**. The Cartesian product is:

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

In other words, the Cartesian product of A and B is the set consisting of all ordered pairs constructed from the elements of both A and B.

Example 3. Let $A = \{a, b, c\}$ and $B = \{c, d\}$. Then:

$$A \times B = \{(a, c), (a, d), (b, c), (b, d), (c, c), (c, d)\}$$

The **power** set of set A, $\mathcal{P}(A)$, is the set consisting of all the subsets of A.

Example 4. Let $A = \{a, b, c\}$. Then $\mathcal{P}(A) = \{\emptyset, a, b, c, \{a, b\}, \{a, c\}, \{b, c\}, A\}$

The number of elements in the power set is always $2^{|A|}$, where $|A|$ denotes the **cardinality**, or number of elements, in A.

Our last definition is that of **Sigma Algebra**, denoted by $\mathcal{F}$. A set of subsets of X is called a Sigma Algebra if the following are satisfied:

- $\emptyset \in \mathcal{F}$

- If $A \in \mathcal{F}$, then $A^c \in \mathcal{F}$
- If $A_1, A_2, \cdots \in \mathcal{F}$, then $\bigcup_{i=1}^{\infty} A_i \in \mathcal{F}$

Example 5. Suppose you toss a coin twice. Then $X = \{HH, TT, HT, TH\}$. Then one possible Sigma Algebra is $\mathcal{P}(X)$. Why? As $\emptyset \in \mathcal{P}(X)$, the complement of any set in $\mathcal{P}(X)$ is also in $\mathcal{P}(X)$, and the union of all the sets in $\mathcal{P}(X)$ is also in $P(X)$.

Logic

Here, I will cover some propositional logic to prepare us for proofs. According to Hammack (2018), logic is "a systematic way of thinking that allows us to parse the meanings of sentences and to deduce new information from old information." As economists, every paper we write will be to deduce new information from old information. Given that most, if not all, of you have taken a logic class at some point, we will review this subject quickly.

To begin logical analysis, we need a **statement**. A statement is a sentence that is either true or false. An example of a statement is "The number 2 is prime." 2 is either prime or not prime, so the statement is either true or false. A non-example is "The integer x is even." The truth of this statement depends on the value of x, so this sentence is not a statement.

Statements can be compound. For example, we can write that "The number 2 is even or the number 3 is odd" (Hammack 2018). Let $P \equiv$ "The number 2 is even" and $Q \equiv$ "the number 3 is odd." Then we can write this statement as $P \vee Q$, where $\vee$ means "or." We can also write that "The number 2 is even and the number 3 is odd." The logical formulation would be $P \wedge Q$, where $\wedge$ means "and." Another statement we can write is "It is not true that the number 2 is even." In logic, we then write $\sim P$, where $\sim$ means "not."

Statements can be conditional. For example, "If I pass my dissertation, I will earn a PhD." Let $P \equiv$ "I pass my dissertation" and $Q \equiv$ "I will earn a PhD." Thus, $P \Rightarrow Q$, or P implies Q. Another way to read this statement is that Q is a **necessary** condition for P, or that P is a **sufficient** condition for Q. Why? Note that for P to be true, Q must be true. But Q being true does not guarantee P is true. But if P is true, Q always follows. A **biconditional** statement is an equivalency. That is, $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. We write this as $P \Leftrightarrow Q$.

We can now derive six common logical inferences with the definitions so far:

Modus Ponens	**Modus Tollens**	**Elimination**
$P \Rightarrow Q$	$P \Rightarrow Q$	$P \vee Q$
P	$\sim Q$	$\sim P$
Q	$\sim P$	Q

Inference 4	**Inference 5**	**Inference 6**
P		
Q	$P \wedge Q$	P
$P \wedge Q$	P	$P \vee Q$

The last bit of notation are **quantifiers**. $\forall$ means "for all" or "for every." $\exists$ means "there exists." Suppose we have a set X. Then I can write "$\exists x \in X$ such that x is odd." Suppose $P(x) \equiv$ "x is odd." Then in logical notation:

$$\exists x \in X, P(x)$$

I can also write "$\forall x \in X$, x is odd." In logic:

$$\forall x \in X, P(x)$$

Now let's look at logical equivalence. To do so, we construct a truth table:

Table 1
Truth Table

P	Q	$\sim P$	$\sim Q$	$P \wedge Q$	$\sim (P \vee Q)$	$\sim P \wedge \sim Q$	$P \Rightarrow Q$	$\sim Q \Rightarrow \sim P$	$P \Leftrightarrow Q$
T	T	F	F	T	F	F	T	T	T
T	F	F	T	F	F	F	F	F	F
F	T	T	F	F	F	F	T	T	F
F	F	T	T	F	T	T	T	T	T

Using the truth table, we can see three laws easily:

(1) Contrapositive: $P \Rightarrow Q = (\sim Q) \Rightarrow (\sim P)$

(2) DeMorgan's Laws: $\sim (P \vee Q) = \sim P \wedge \sim Q$ **and** $\sim (P \wedge Q) = \sim P \vee \sim Q$

(3) Commutative Laws: $P \wedge Q = Q \wedge P$ **and** $P \vee Q = Q \vee P$

Two other laws you can verify using truth tables include:

(4) Distributive Laws: $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$ **and** $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$

(5) Associative Laws: $P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$ **and** $P \vee (Q \vee R) = (P \vee Q) \vee R$

While we will rarely use formal logic like truth tables, the laws of logic will be useful in proving statements and conducting research.

Proof

In this section, I will briefly cover the basic methods of mathematical proof. In all proofs, we are looking to show that a conditional statement is either true or false.

Direct Proof

We first revisit the truth table:

Table 2
Direct Proof Truth Table

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Note that when P is false, the conditional statement is automatically true. When proving this statement then, we need to focus on the cases when P is true. In **direct** proof, we do this by assuming P is true at the outset of our argument. An example taken from Hammack (2018) but written in my words is below:

Claim: If x is odd, x^2 is odd.

Proof. Suppose x is odd. Then by the definition of an odd number, $x = 2a + 1$ where $a \in \mathbb{Z}$. Squaring both sides of the equation gives:

$$\begin{aligned} x^2 &= (2a+1)^2 \\ &= 4a^2 + 4a + 1 \\ &= 2(2a^2 + 2a) + 1 \end{aligned}$$

Let $b = 2a^2 + 2a$. Note that $b \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under addition and multiplication. Then:

$$x^2 = 2b + 1$$

But this is the definition of an odd number, thus proving the claim. ■

Proof by Cases

Sometimes, we need to examine multiple cases in a direct proof. An example from Hammack (2018) follows:

Claim: If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Proof. Suppose that $n \in \mathbb{N}$. There are two cases here: n is either even or odd.

Case 1: Suppose n is even. Then by the definition of an even number, $n = 2a$, for some $a \in \mathbb{Z}$. We then know that $(-1)^n = 1$. Therefore:

$$\begin{aligned} 1 + (-1)^n(2n-1) &= 1 + (2 * (2a) - 1) \\ &= 1 + 4a - 1 \\ &= 4a \end{aligned}$$

This is a multiple of 4, so case 1 is verified.

Case 2: Suppose n is odd. Then by the definition of an odd number, $n = 2b + 1$, for some $b \in \mathbb{Z}$. We then know that $(-1)^n = -1$. Therefore:

$$\begin{aligned} 1 + (-1)^n(2n - 1) &= 1 - (2 * (2a + 1) - 1) \\ &= 1 - (4a + 2 - 1) \\ &= 1 - (4a + 1) \\ &= -4a \end{aligned}$$

This is a multiple of 4, so case 2 is verified.

Since both cases are true, we have shown the claim is true. ■

Proof by Contrapositive

Recall that the law of contrapositive says that $P \Rightarrow Q$ is the same as $\sim Q \Rightarrow \sim P$. In a proof by **contrapositive**, we will prove that $P \Rightarrow Q$ by proving $\sim Q \Rightarrow \sim P$. Consider the example from Hammack (2018) below:

Claim: Suppose $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd.

Proof. (by Contrapositive) Suppose that x is *not* odd. That is, suppose x is even. Then by the definition of an even number, $x = 2a$ for some $a \in \mathbb{Z}$. Thus:

$$\begin{aligned} 7x + 9 &= 7(2a) + 9 \\ &= 14a + 9 \\ &= 2(7a + 4) + 1 \end{aligned}$$

Let $b = 7a + 4$. Note that $b \in \mathbb{Z}$ by closure of $\mathbb{Z}$ under addition and multiplication. Then:

$$7x + 9 = 2b + 1$$

But this is the definition of an odd number. This verifies the contrapositive, proving the original claim. ■

Proof by Contradiction

We didn't build a truth table for contradiction before, so let's do so now. Suppose P is some conditional statement and C is a result that we can derive from P. Then:

Table 3
Contradiction Truth Table

P	C	$C \wedge \sim C$	$\sim P \Rightarrow (C \wedge \sim C)$
T	T	F	T
T	F	F	T
F	T	F	F
F	F	F	F

Strangely enough, by showing that not P implies a **contradiction** (both C and not C at the same time), we can prove the original conditional statement. Below is an example:

Claim: $\nexists a, b \in \mathbb{Z}$ such that $18a + 6b = 1$.

Proof. (by Contradiction) Suppose $\exists a, b \in \mathbb{Z}$ such that $18a + 6b = 1$. Then:

$$18a + 6b = 1$$
$$3a + b = \frac{1}{6}$$

By closure of $\mathbb{Z}$ under addition and multiplication, $3a+b \in \mathbb{Z}$. But $\frac{1}{6} \notin \mathbb{Z}$. $3a+b$ cannot be both an element of $\mathbb{Z}$ and not an element of $\mathbb{Z}$. This is a contradiction. Therefore, the claim is true. ■

Proof by Induction

Sometimes to prove a statement, we need **induction**. We first show that a base case is true. After that, we can use the base case to show that the statement is always true. An example:

Claim: If $n \in \mathbb{N}$, then $1 + 3 + 5 + 7 + \cdots + (2n - 1) = n^2$.

Proof. (by Induction) Suppose that $n \in \mathbb{N}$.

Base Case: Let $n = 1$. Then $1 = 1^2$. The claim holds.
Inductive Step: Now we show that because the claim holds for k, it also holds for $(k+1)$. Suppose that $1 + 3 + 5 + 7 + \cdots + (2k-1) = k^2$. Then:

$$\begin{aligned} 1 + 3 + 5 + 7 + \cdots + (2(k+1) - 1) &= 1 + 3 + 5 + 7 + \cdots + (2k-1) + (2(k+1) - 1) \\ &= k^2 + 2k + 2 - 1 \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

This verifies the inductive step, so the claim is true. ■

Disproof

Technically, there are many forms of disproof, but we will very briefly cover **direct disproof**. To disprove the claim $P \Rightarrow Q$, we simply show that $P \not\Rightarrow Q$. Below is an example:

Claim: For every $n \in \mathbb{Z}$, $f(n) = n^2 - n + 11$ is prime.

Disproof. To disprove the claim, we need to find an $n \in \mathbb{Z}$ such that $f(n)$ is not prime. Consider the below table:

Table 1
Truth Table

n	0	1	2	3	4	5	6	7	8	9	10	11
$f(n)$	11	11	13	17	23	31	41	53	67	83	101	121

$n = 11$ disproves the claim, as 121 is not a prime number. ■

Proof of the Partitioning Theorem

In sets we covered one theorem, which we will now prove.

Theorem 2 (Partitioning Theorem)**.** *If $\{B_1, B_2, \dots\}$ is a partition of X, then for any set A:*

$$A = \bigcup_{i=1}^{\infty} A \cap B_i$$

and the sets $(A \cap B_i)$ *are mutually disjoint.*

Proof. Take any element $a \in A$. Because $\{B_1, B_2, \dots\}$ is a partition of X, $a \in B_i$ for some i. Therefore, $a \in A \cap B_i$ for some i. But if $a \in A \cap B_i$, then $a \in \bigcup_{i=1}^{\infty} A \cap B_i$. So $a \in A \Rightarrow a \in \bigcup_{i=1}^{\infty} A \cap B_i$.

Now take an element $b \in \bigcup_{i=1}^{\infty} A \cap B_i$. Because B_i is mutually disjoint, $b \in A \cap B_i$ for some i. By the definition of $\cap$, $b \in A$. Therefore, $b \in \bigcup_{i=1}^{\infty} A \cap B_i \Rightarrow b \in A$.

These two cases prove that $A = \bigcup_{i=1}^{\infty} A \cap B_i$. ■