Proof Workshop Week 1: Logic and Set Theory

September 15, 2023

Contents

1 Day 1: Logic and Set Theory

Our goal in this workshop is to introduce you to and allow you to practice proofwriting. The specific topic today is logic and set theory, but the content itself isn't nearly as important as learning about different types of proof strategies, practicing these strategies, and getting feedback on your work. Thus although some of you will already be familiar with the logic and set theory we'll cover (especially those taking courses such as Honors Math, Modern Algebra I, or Analysis I), you can still get a lot of proofwriting practice out of today.

Over the next few weeks, we'll start to cover more interesting and advanced topics. Here's the outline of the coming weeks:

- Day 1. Logic and Set Theory
- Day 2. Proof Types and Strategies: Contradictions, Contrapositives, and Induction (and when to use them!)
- Day 3. Intro to Algebraic Reasoning: The Integers and Peano Arithmetic
- Day 4. Intro to Analytic Reasoning: Limits, Continuity, and $\epsilon - \delta$ Proofs

Beyond just practicing these ideas, it's extremely important to get feedback on what you've practiced. At the end of every workshop, we'll collect your solutions to a couple of problems and return them to you with feedback from our TAs. Problems which we will collect are marked with the ($\bigstar$) symbol; you should attempt these fairly early on so that you're done when we collect them. Don't worry if you don't finish these—partial solutions will be accepted.

1.1 Logic

Mathematical proofs use certain vocabulary to structure the arguments and communicate more effectively with any reader who is familiar with the language. We'll start by familiarizing ourselves with common terms:

- Theorem: A substantial mathematical statement which has been proven to be true.
- Corollary: A consequence of a theorem which follows either immediately from it or from the theorem combined with other established facts.
- Lemma: A smaller statement that needs to be proved as an intermediate step to proving a theorem.
- Proposition: A mathematical statement which should be proven to be true.
- Definition: The meaning of a new term.
- Proof: A series of logical steps that shows that establishes the validity of a claim
- Axiom: A statement that one takes as a given and cannot be proved.

The line between theorem, corollary, lemma, and proposition is murky, and people will often say label the same statements as different things. A proposition is more general than all of the others: they are examples of propositions that we label as having varying levels of important with language. Axioms are the starting point of reasoning; we will talk more about axioms on Day 3.

1.1.1 Propositional logic

Definition 1.1. A **propositional statement** is a statement that is either true or false.

These are usually denoted P or Q. If P or Q depends on some variable x, we may denote them $P(x)$ or $Q(x)$.

Example 1.2. The statement $P =$ "all dogs have white fur" is false and the statement $Q =$ "5 is an odd integer" is true. The statement $P(x) =$ "x is Sunday" depends on the value of the variable x.

We can combine propositional statements with *connective symbols*. Here are the three main ones:

Definition 1.3. 1. Write $P \vee Q$ to stand for the statement "P or Q".

2. Write $P \wedge Q$ to mean "P and Q".

3. Write $\neg P$ to mean "Not P". $\neg P$ always has the opposite truth value of P.

Remark 1.4. The $\vee$ operator is an "inclusive or". $P \vee Q$ means that either P is true, Q is true, or both are true.

Remark 1.5. We can write propositional statements as **truth tables**. Here are examples for the operations we just defined:

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

These logical operations obey the **distributive law**:

$$P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$$
$$P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$$

and **De Morgan's laws**:

$$\neg(P \wedge Q) \iff \neg P \vee \neg Q$$
$$\neg(P \vee Q) \iff \neg P \wedge \neg Q$$

Definition 1.6. Let P, Q be propositional statements. The proposition "if P, then Q", denoted $P \implies Q$, has the truth table:

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

We call P the **hypothesis** and Q the **conclusion**.

Definition 1.7. 1. If $P \implies Q$ and $Q \implies P$, then we say "P **if and only if** Q" and write $P \iff Q$.

2. The **converse** of $P \implies Q$ is the statement $Q \implies P$.

3. The **contrapositive** of $P \implies Q$ is the statement $\neg Q \implies \neg P$.

Example 1.8. Here are two true statements about the real numbers:

1. If $x > 0$, then $x^3 \neq 0$.

2. If $x^2 < 0$, then $x = 23$.

In every case in which the hypothesis holds, the conclusion holds as well. Of course, in case (2) there are no cases where the hypothesis holds. Statements like this are called **vacuously true**.

Definition 1.9. Two propositional statements are **logically equivalent** if one is true if and only if the other is true.

1.1.2 Quantifiers and Predicate logic

We often want to say that a certain property is true for all or at least one element of a set. We will do this through quantifiers.

Definition 1.10. Let $P(x)$ be a proposition depending on $x \in S$ for S a set.

1. If $P(x)$ is true for every value of x in S, then we write $\forall x \in S, P(x)$. This is read "for all x in S, $P(x)$". $\forall$ is called the **universal quantifier**.
2. If $P(x)$ is true for at least one element $x \in S$, then we write $\exists x \in S, P(x)$ and say "there exists x in S such that $P(x)$". $\exists$ is the **existential quantifier**.

Example 1.11. The order of quantifiers matter. Consider the two statements below. Which is true and which is false?

1. $\forall\, x \in \mathbb{Z},\ \exists\, y \in \mathbb{Z}\,(2x - y = 0)$
2. $\exists\, x \in \mathbb{Z},\ \forall\, y \in \mathbb{Z}\,(2x - y = 0)$

1.1.3 Exercises

1. Write the following sentences in symbolic form:
   a) There is a number which when multiplied with any other number, results in the original number.
   b) Every number has another number which squares to it.
2. $P(x) =$ "x has at least 3 distinct prime factors", $Q(x) =$ "$x \geq 20$". Which of $P \implies Q$, $Q \implies P$, $P \iff Q$ are true?
3. Write the contrapositive and converse of the following statement: "If $x < 0$, then $x^2 - x > 0$" and determine which (if any) of the three statements are true.
4. Let A and B be sets of real numbers. Write the negation of the following statements:
   a) For every $a \in A$, it is true that $a^2 \in B$
   b) For at least one $x \notin A$, it is true that $a^2 \in B$
5. Show De Morgan's Law by writing a truth table:
   a) $\neg(P \wedge Q) \iff \neg P \vee \neg Q$
   b) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$
6. Prove the distributive law:
   a) $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$
   b) $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$
7. (Hard!) Define two operators XOR and NAND with the truth tables below:

P	Q	P XOR Q	P NAND Q
T	T	F	T
T	F	T	T
F	T	T	T
F	F	F	F

   a) Construct the XOR operation from $\wedge, \vee, \neg$

b) Using only the NAND operation, construct the operators $\neg, \vee, \wedge$.

c) Formulate a "not-or" operation NOR and construct it using $\neg, \vee, \wedge$.

d) Using only the NOR operation, construct the operators $\neg, \vee, \wedge$.

The exercise above gives some examples of important logic gates. Part (b) and (c) show that NAND and NOR are **functionally complete**: every possible logic gate can be assembled only from NAND gates, or NOR gates. This is important in computer science.

Try to construct a proposition that does the 'xor' operation. (outputs True if and only if one of P and Q is true).

"nand" generates "not", "and", "or"

1.2 Set Theory

1.2.1 Sets

Sets are the foundation of mathematics.

Definition 1.12. A **set** is a collection of objects, not allowing for repeats.

We indicate that an object is a set by writing two brackets $\{\}$ with something in the middle.

Example 1.13. 1. The set consisting of the numbers 1, 2, and 3 is a set, written $\{1, 2, 3\}$.

2. The set of all students in the class is a set.

3. The set of all integers is a set, denoted $\mathbb{Z}$.

4. The set of all real numbers is a set, denoted $\mathbb{R}$.

Definition 1.14. The objects contained in a set are called its **elements**. If an object x is an element of a set S, we write $x \in S$.

Conversely, if an object x is **not** an element of a set S, we write $x \notin S$.

Example 1.15. We write $1 \in \{1, 2, 3\}$, $2 \in \{1, 2, 3\}$, and $3 \in \{1, 2, 3\}$.

We say that two sets are **equal** if they have precisely the same elements.

There is one particular set which shows up throughout mathematics and deserves its own name.

Definition 1.16. The **empty set**, written $\emptyset$ is the set with no elements.

Beyond saying what a set contains, we also have a way of comparing what two sets contain.

Definition 1.17. Suppose we have two sets S and T. If all of the elements of S are contained in T, we say S is a **subset** of T, and write $S \subset T$. If $S \subset T$ and $S \neq T$, we call S a **strict subset** of T, and write $S \subsetneq T$.[1]

[1] Confusingly, it is also common to see $S \subseteq T$ mean "S is a subset of T" and $\subset$ mean "S is a strict subset of T".

As with elements, if S is **not** a subset of T, we write $S \not\subset T$.

Example 1.18. 1. We have $\{1,2\} \subset \{1,2,3\}$.

2. We also have $\{1,2,3\} \subset \mathbb{Z}$.

3. For any set S, we have $\emptyset \subset S$.

Sometimes, we wish to define a subset S of a set T which consists of precisely the elements x which satisfy a property P. We write

$$S = \{x \in T \mid P(x)\}$$

This is called **set builder notation**. [2]

Example 1.19. The set of even integers can be written as

$$\{n \in \mathbb{Z} \mid n \text{ is even}\}.$$

In the same way that there are the addition and multiplication operations that we do on numbers, there are two key operations we can do on sets.

Definition 1.20. Let S and T be sets.

- The **union** of S and T, written $S \cup T$, is the set of all elements contain in either S or T (in set builder notation, $S \cup T = \{x : x \in S \vee x \in T\}$).
- The **intersection** of S and T, written $S \cap T$, is the set of all elements contain in either S or T (in set builder notation, $S \cap T = \{x : x \in S \wedge x \in T\}$).
- The **difference** between two sets S and T, written $S \setminus T$, is the set of all elements in S not contained in T (in set builder notation, $S \setminus T = \{x \in S : x \notin T\}$.

Remark 1.21. Union and intersection are *commutative*, which means that $S \cup T = T \cup S$ and $S \cap T = T \cap S$. Set difference, on the other hand, is not: usually, $S \setminus T \neq T \setminus S$.

1.2.2 Functions

Definition 1.22. A **function** f from a set S to a set T is a rule which assigns every element of S to an element of T. We write $f : S \to T$. We call S the **domain** of f and T the **co-domain** of f. Given an element $x \in S$, we write $f(x)$ for the element of T which f assigns to it.

In particular, a function isn't just the rule itself f itself, but the rule together with two sets, the domain and co-domain.

Example 1.23. 1. Familiar functions such as $f(x) = x^2$ and $g(x) = \sin(x)$ are all functions from $\mathbb{R}$ to $\mathbb{R}$.

2. We could also define a function $h : \mathbb{R}_{\geq 0} \to \mathbb{R}$ given by $h(x) = x^2$, where $\mathbb{R}_{\geq 0}$ denotes the set of real numbers greater than or equal to 0. Although f and h satisfy the same "formula", they are different functions, as they have different domains.

[2] Sometimes, when we want to consider *all* objects which satisy a property P, we write $\{x \mid P(x)\}$ for this set. However, for technical reasons, this set may not actually exist! Consequently, this notation should mostly be avoided.

3. Not every function needs to be written as a “formula”. For instance, we could define a function $r : \{1, 2, 3\} \to \{\text{cow}, \text{pig}\}$ as follows:

x	$f(x)$
1	cow
2	pig
3	cow

The case of f and h in Example 1.23 highlights another important attribute of functions.

Definition 1.24. Let $f : S \to T$ and $A \subset S$. The **restriction** of f to A, written $f \upharpoonright A$ or $f \upharpoonright_A$, is a function $f \upharpoonright A : A \to T$ given by the same rule as f, but with domain A.

Example 1.25. The functions $f : \mathbb{R} \to \mathbb{R}$ and $h : \mathbb{R}_{\geq 0} \to \mathbb{R}$ given by $f(x) = h(x) = x^2$ from Example 1.23 are an example of a restriction: in particular, $h = f|\mathbb{R}_{\geq 0}$

Sometimes, when we want a function to be defined by multiple “formulas”, we write it **piecewise**; for instance, the function r from Example 1.23 can be rewritten as

$$r(x) = \begin{cases} \text{cow} & x = 1 \vee x = 3 \\ \text{pig} & x = 2 \end{cases}$$

Definition 1.26. Let $f : S \to T$. We say f is **injective** if whenever $f(x_1) = f(x_2)$, we have $x_1 = x_2$.

Definition 1.27. Let $f : S \to T$. We say f is **surjective** if for every $y \in T$, there exists an $x \in S$ such that $f(x) = y$.

Definition 1.28. If $f : S \to T$ is both injective and surjective, we say it is a **bijection** between S and T.

Example 1.29. The function $h : \mathbb{R}_{\geq 0} \to \mathbb{R}$ given in Example 1.23 as $h(x) = x^2$ is an example of an injection but not a surjection, since negative numbers don’t have real square roots. Note that the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is **not** an injection, since $-x$ and x map to the same element x^2. This exhibits the need to consider the domain and codomain as part of the data of a function.

Example 1.30. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^3$ is a bijection.

1.2.3 Exercises

We begin with an example of a proof using sets.

Proposition 1.31. For any sets A, B, and C, we have

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

This is an analogue of the distributive law.

Proof. For notational convenience, write $E = A \cap (B \cup C)$ and $F = (A \cap B) \cup (A \cap C)$. Suppose $x \in E$. Then $x \in A$ and $x \in B \cup C$, which means $x \in B$ or $x \in C$ (and possibly both). Then either $x \in A \cap B$ or $x \in A \cap C$, so $x \in F$. It follows that $E \subset F$.

Now suppose $x \in F$. Then $x \in A \cap B$ or $x \in A \cap C$. Then we must have $x \in A$, and either $x \in B$ or $x \in C$. Thus $x \in E$, so $F \subset E$. Since $E \subset F$ and $F \subset E$, we know that $E = F$. □

The above argument is called a **double containment** argument, and illustrates the general approach of showing that two sets A and B are equal by showing that $A \subset B$ and $B \subset A$.

1. (Basic properties of unions, intersections, and complements) Let A, B, C be sets. Prove the following statements:

   a) $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$.

   b) Let $A \subset X$. Then $A \cup X = X$ and $A \cap X = A$.

   c) $A \cup (B \cap C) = (A \cup B) \cap (A \cup B)$. This is another analogue of the distributive law.

2. (Set Complements and De Morgan's Law). Let X, A, B be sets. We define the *complement of* A *in* X as the set $X \setminus A = \{x \in X \mid x \notin A\}$. Some people also write this as $X - A$. Note that $X \setminus A = X$ if $A \not\subset X$.

   a) Show that $A \cup (X \setminus A) = X$ and $A \cap (X \setminus A) = \emptyset$.

   b) Show *De Morgan's laws* for sets: we have $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$ and $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$

   c) Suppose $A \cup B = X$ and $A \cap B = \emptyset$. Show that $A = X \setminus B$ and $B = X \setminus A$.

3. We say a function $f : X \to Y$ has an **inverse** g if $g(f(x)) = x$ and $f(g(y)) = y$ for any $x \in X$ and $y \in Y$. We write $g = f^{-1}$.

   Show that f is a bijection if and only if it has an inverse.

4. Let $f : X \to Y, g : Y \to Z$ be functions.

   a) Show that if f and g are both injective, then so is $g \circ f$.

   b) Show that if f and g are both surjective, then so is $g \circ f$.

5. (★) Let $f : X \to Y, g : Y \to Z$ be functions.

   a) Suppose that $g \circ f$ is injective. Show that f is injective, and give an example which shows that g need not be.

   b) Suppose that $g \circ f$ is surjective. Show that g is surjective, and give an example which shows that f need not be.

6. Let $f : X \to Y, \tilde{f} : X \to Y, g : Y \to X, \tilde{g} : Y \to X$ be functions.

   a) Show that if $g \circ f = g \circ \tilde{f}$ and g is injective, then $f = \tilde{f}$.

   b) Give an example where (a) fails when g is not injective.

   c) Show that if $g \circ f = \tilde{g} \circ f$ and f is surjective, then $g = \tilde{g}$.

   d) Give an example where (c) fails when f is not surjective.

7. Let $f : X \to Y$ and let $B \subset Y$. The **preimage** of B under f is the set $f^{-1}(B) = \{x \in X : f(x) \in B\}$.[3]

   When B is a singleton $\{y\}$, we often write $f^{-1}(y)$ for $f^{-1}(\{y\})$ for simplicity.

[3] Although the preimage uses the same notation as an inverse, a function does not need to be a bijection for the preimage to be defined! For example, if $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = x^2$, then $f^{-1}(\{4\}) = \{2, -2\}$.

a) If $f : X \to Y$ and $B_1, B_2 \subset Y$, show that $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

b) If $f : X \to Y$ and $B_1, B_2 \subset Y$, show that $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

The fact that the preimage of a function preserves intersection and union (and, in fact, complements) will be of fundamental importance to the field of topology. The image of a function doesn't always preserve interesection, union, and complement like this; think about why and come up with an example.

1.3 Direct Proofs

1.3.1 Exercises

1. Recall that the **power set** of a set X is the set of subsets of S: $\{A : A \subset X\}$. It is denoted $P(X), \mathcal{P}(X)$, and 2^X, among other things.

   If X has two elements, show that $\mathcal{P}(X)$ has four elements. Show that if X has three elements then $\mathcal{P}(X)$ has 8 elements. In general, if X has n elements, how many elements does $\mathcal{P}(X)$ have?

2. An integer n is **even** if there exists an integer k such that $n = 2k$. An integer n is **odd** if there exists an integer k such that $n = 2k + 1$. Show that:

   a) The sum of two odd numbers is even.

   b) The sum of two even numbers is even.

   c) The sum of an odd number and an even number is odd.

   d) If n is even, so is n^2.

   e) If x and y are integers and $x^2 + y^2$ is even, then $x + y$ is even.

3. If $n \neq 0$ and a are integers, we say n **divides** a or $n \mid a$ if there exists an integer m such that $a = nm$.

   a) If m divides a and n divides b, then mn divides ab.

   b) Let n be an integer and let (n) be the set of multiples of n, i.e. $(n) = \{a : a \text{ divides } n\}$. Show that if $a, b \in (n)$ and x and y are any integers, then $ax + by \in (n)$.

4. Let $n = 4k_1 + 1$ and $m = 4k_2 + 1$. Show there exists k_3 such that $nm = 4k_3 + 1$.