Proof Workshop

Contents

1 Week 1: Logic and Proof Strategies

1.1 Introduction

Roughly speaking, a proof is a sequence of mathematical statements $P_0, \ldots, P_n$ such that each P_i is either an *assumption,* i.e. some fact which is already known, or can be derived from the previous statements via a logical rule. The goal of this workshop is to introduce the basics of mathematical proof and to give you the opportunity to practice proofwriting. In particular, we will:

- Become familiar with the conventions pertaining to the syntax of proofwriting, including the language and notation common to all mathematical proofs.
- Learn common rules of inference and the role of logic in mathematical proofs.
- Practice identifying the assumptions inherent in any mathematical argument.

It is of utmost importance to practice the content we will introduce and to get feedback on your work. Although some of you will already be familiar with the material we'll cover (especially those taking courses such as Honors Math, Modern Algebra I, or Analysis I), you should still be able to extract a lot of value from the workshop.

Here's the outline of the coming weeks:

- Day 1. Logic and Proof Strategies: Direct Proof, Proof by Contrapositive, and (Dis)Proof by Counterexample
- Day 2. Proof Strategies (cont.): Proof by Contradiction and the Principle of Mathematical Induction.
- Day 3. Set Theory: Sets, Relations, and Functions.
- Day 4. Analytic Reasoning: Limits, Continuity, and ϵ-δ Proofs
- Day 5. More on Set Theory: Equivalence Relations and Cardinality.

At the end of every week, we will provide you with a problem set pertaining to the content of the lecture. Write solutions to a couple of problems and submit them for your TAs for feedback. Don't worry if you don't finish them—the course is not graded, and we will still give feedback on partial solutions.

1.2 Logic

1.2.1 Propositional calculus

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

Example 1.2. The statement $P =$ "all dogs have white fur" is false and the statement $Q =$ "5 is an odd integer" is true.

Remark 1.3. Sometimes, the truth value of a propositional statement depends on a **variable.** To express the dependence of a statement on a variable x, we will write $P(x)$. If P depends on both x and y, we will write $P(x, y)$, and so on. A propositional statement which depends on one or more variables is also known as a **predicate.**

Example 1.4. The statement $P(x) =$ "$x \geqslant 5$" is true or false according to the value of x. The statement $P(x, y) =$ "$x + y = 2$" depends on both x and y. Similarly, the statement $R(x, y) =$ "$x \geqslant y$" also depends on both x and y.

The rules of propositional logic decide whether an argument is valid. Consider the following example.

- It is raining or snowing.
- It is not snowing.
- Therefore, it is raining.

If we let P be the statement that "it is raining," and Q be the statement that "it is snowing," the argument can be written in symbolic form as follows:

- P or Q.
- Not Q.
- Therefore, P.

The statements "P or Q" and "not Q" are called the **hypotheses** of the argument, while P is called the **conclusion.**

As the example above suggests, we can combine propositional statements to produce new propositional statements via logical connectives like "and," "or," and "not."

Definition 1.5.

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

Remark 1.7. The effect of these operations on truth values is catalogued by a so-called truth table, shown in Table 1.

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

Table 1: Some basic logical operations.

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

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

and **De Morgan's laws**:

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

These identities can be derived by examining truth tables; examples are given in the exercises.

Another way of combining two propositional statements is via a conditional.

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

Table 2: Truth table of $P \Rightarrow Q$.

Definition 1.8. Let P, Q be propositional statements. The proposition "if P, then Q," denoted $P \Rightarrow Q$, has the truth table given in Table 2.

Example 1.9. The statement $P(x) =$ "If x is an even integer, then x^2 is an even integer" is true. The statement $Q =$ "If it rains on a Friday, then it must rain the Friday after that" is false.

Remark 1.10. Note that if P is false, then "$P \Rightarrow Q$" is true. This is known as *vacuous truth.*

Remark 1.11. If you check the truth tables (or better, if you really think it through), you will see that $P \Rightarrow Q$ has the same truth table as $\neg P \vee Q$. The intuition behind this equivalence is that P forces Q to be true: Q can be true regardless of the value of P, but if P is true, then Q must also be true for the statement to hold.

Definition 1.12.

1. If $P \Rightarrow Q$ and $Q \Rightarrow P$, then we say "P **if and only if** Q" and write $P \iff Q$.
2. The **converse** of $P \Rightarrow Q$ is the statement $Q \Rightarrow P$.
3. The **contrapositive** of $P \Rightarrow Q$ is the statement $\neg Q \Rightarrow \neg P$. Note that the contrapositive has the same truth table. Thus,

$$(P \Rightarrow Q) \iff (\neg Q \Rightarrow \neg P).$$

Definition 1.13. Two propositional statements are **logically equivalent** if one is true if and only if the other is true.

Hence, a conditional and its contrapositive are logically equivalent.

1.2.2 Valid Arguments

We say that an argument is *valid* if, when reduced to symbolic form, the conclusion is always true when the hypotheses are true. In other words, the argument is valid if the conclusion can only be true if the hypotheses are true, "according to the rules of logic."

Going back to our previous example, the argument

- $P \vee Q$.
- $\neg Q$.
- Therefore, P.

is valid; if we look at the truth table, $P \vee Q = 1$ and $\neg Q = 1$ means that the only possibility for P is $P = 1$. However, consider the following argument:

- $x \geqslant 5$.
- $5 \geqslant 3$.
- Therefore, $x \geqslant 3$.

While the conclusion of the argument is correct, the argument itself is not valid. Written in symbolic form, we can write this argument as

- $R(x, 5)$.
- $R(5, 3)$.
- Therefore, $R(x, 3)$.

From this, we see that the argument is missing a crucial hypothesis, that $R(x, 5) \wedge R(5, 3) \Rightarrow R(x, 3)$. In other words, we have implicitly assumed in the argument itself that $\geqslant$ is transitive.

On the other hand, the following argument is totally valid, even though the conclusion is absurd.

- Butterball ate a pig.
- If anything eats a pig, they become a pig.
- Therefore, Butterball became a pig.

It is very easy to make hidden assumptions which are not presented to you, on the pretense that they are "obvious." The purpose of familiarizing yourself with the rules of propositional logic is to know, with certainty, when a particular argument is valid when all of the assumptions given are laid out.

1.2.3 Quantifiers

There is another way in which we can create new propositional statements from old which we have not yet introduced. This is done via **quantifiers.**

Definition 1.14. Let $P(x)$ be a proposition depending on x.

1. We say that $\exists x : P(x)$ is true if there **exists** some x such that $P(x)$ is true.
2. We say that $\forall x : P(x)$ is true if $P(x)$ is true **for all** x.

$\exists$ is called the **existential quantifier** and $\forall$ is called the **universal quantifier.**

Example 1.15. $\forall x : x \geqslant 2$ is false, while $\exists x : x \geqslant 2$ is true.

Most of the time, we will preface an $\exists$ or $\forall$ quantifiers as ranging over all x in a certain set (which you can think of as just a collection of objects). For example, $\forall x \in \mathbb{N}$ means "for every natural number x," whereas $\exists x \in \mathbb{N}$ means "there exists a natural number x."

Example 1.16. 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. $\exists x \in \mathbb{Z} : (\forall y \in \mathbb{Z} : (2x - y = 0))$

Remark 1.17. Often, statements like $\exists x : P(x)$ are written $\exists x P(x)$, so statements with mixed quantifiers are often written $\forall x \exists y P(x, y)$. This is an abbreviation of $\forall x : (\exists y : P(x, y))$.

The last logical rule we introduce has to do with negating quantifiers. Negating an existential quantifier transforms it into a universal one, and vice versa:

$$\neg(\exists x : P(x)) \iff \forall x : \neg P(x), \quad \neg(\forall x : P(x)) \iff \exists x : \neg P(x).$$

Example 1.18. Analyze the logical form of the following statement: "Nobody likes a sore loser." Using $L(x, y)$ to mean "x likes y" and $S(x)$ to mean that "x is a sore loser," the statement can be interpreted as:

$$\forall x : \neg(\exists y : S(x) \wedge L(y, x)) = \forall x \forall y (\neg S(x) \vee \neg L(y, x)),$$

or in words: "for all x, it is not true that there is a y such that x is a sore loser and y likes x." We can also think about this statement in this way: "for all y, if x is a sore loser, then y does not like x." In symbols:

$$\forall y : (\forall x : S(x) \Rightarrow \neg L(y, x)).$$

From the identity $P \Rightarrow Q = \neg P \vee Q$, we see this is the same as

$$\forall y \forall x (\neg S(x) \vee \neg L(y, x))$$

which is the same as what we got earlier.

1.3 Proof Strategies

1.3.1 Direct Proofs

Let's begin proving things. A **direct proof** is a basic technique used to prove conditional statements, i.e. statements of the form $P \Rightarrow Q$. Many mathematical statements are of this form (although not all).

$P \Rightarrow Q$ can only be false if P is true and Q is false. To prove this statement, then, we only need to consider the case where P is true. A direct proof of $P \Rightarrow Q$ thus proceeds as follows:

- Suppose P.
- $\cdots$
- Therefore, Q.

Before we start giving examples, let's begin with a basic definition.

Definition 1.19. 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 $n = 2k + 1$.

Example 1.20. If x is an odd integer, then x^2 is an odd integer.

Proof. Suppose x is odd. By definition, there exists an integer k such that $x = 2k + 1$. Then $x^2 = (2k + 1)^2 = 4k^2 + 2k + 1$. Since $4k^2 + 2k + 1 = 2(2k^2 + k) + 1$ and $2k^2 + k$ is an integer, we have $x^2 = 2k' + 1$ for the integer $k' = 2k^2 + k$. Thus, by definition, x^2 is odd. □

Remark 1.21. Generally, when mathematicians state theorems which are dependent on some variable x, they mean to say that the theorem is true $\forall x$. Thus, to prove the theorem "If x is an odd integer, then x^2 is an odd integer," we really have to prove the propositional statement

$$\forall x : (x \text{ is an odd integer} \Rightarrow x^2 \text{ is an odd integer}).$$

Thus, such a proof for $\forall x : P(x) \Rightarrow Q(x)$ would start by choosing an arbitrary x which satisfies $P(x)$, then proving that $Q(x)$ is true.

Example 1.22. If x and y are odd integers, then xy is an odd integer.

Proof. Suppose x and y are odd integers. By definition, $x = 2k + 1$ and $y = 2k' + 1$ for some integers k, k'. Then $xy = (2k+1)(2k'+1) = 4kk'+2k+2k'+1 = 2(2kk'+k+k')+1$. Because $2kk' + k + k'$ is an integer, we have $xy = 2a+1$ for the integer $a = 2kk' + k + k'$. Thus, by definition, xy is odd. □

1.3.2 Proof by Contrapositive

Another common proof strategy is the **proof by contrapositive**. Suppose we want to prove $P \Rightarrow Q$. As we noted above, this is equivalent to the statement $\neg Q \Rightarrow \neg P$.

One way to be convinced of this is to remember that $P \Rightarrow Q$ is the same as $\neg P \vee Q$. If we rewrite $\neg Q \Rightarrow \neg P$ in this way, we get

$$\begin{aligned} \neg Q \Rightarrow \neg P &\iff \neg(\neg Q) \vee \neg P \\ &\iff Q \vee \neg P \\ &\iff \neg P \vee Q \\ &\iff P \Rightarrow Q. \end{aligned}$$

When giving a proof of the contrapositive, we often say "we will prove the contrapositive" or say "assume $\neg P$" to indicate we are doing so.

We often want to use the contrapositive when it is easier to work with the statement $\neg Q$ than the statement P. We give a few examples below.

Example 1.23. If $x^2 - 6x + 5$ is even, then x is odd.

Proof. Suppose x is not odd, so that it is even and $x = 2a$ for some integer a. Then

$$x^2 - 6x + 5 = (2a)^2 - 6(2a) + 5 = 4a^2 - 12a + 5 = 4a^2 - 12a + 4 + 1 = 2(2a^2 - 6a + 2) + 1.$$

Therefore, $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2$. Thus $x^2 - 6x + 5$ is not odd, and so it must be even. □

Remark 1.24. You may have noticed that we have made a hidden assumption, that every integer is either odd or even. With our definition of even and odd, it is not obvious that this is the case. You will have the opportunity to prove this in the problem sets after we have discussed induction, but for now, we will just assume that it is true.

If we were to prove the above directly, we would begin by assuming $x^2 - 6x + 5$ is even, so $x^2 - 6x + 5 = 2a$. But then it is not clear where to proceed, since we would need to isolate x from the quadratic equation. But with the contrapositive, the proof reduces to a calculation.

Remember that when negating a statement you may need to use DeMorgan's law. First, a definition.

Definition 1.25. If a and b are integers with $a \neq 0$, we say that a **divides** b, or that b is **divisible by** a, if there exists an integer k such that $b = ka$. In this case, we write $a \mid b$.

Example 1.26. Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Proof. Suppose it is not true that $5 \nmid x$ **and** $5 \nmid y$. Then $5 \mid x$ **or** $5 \mid y$. Suppose $5 \mid x$. Then $x = 5a$ for some integer a and then $xy = (5a)y$ and so 5 divides xy. Similarly if 5 divides y then $y = 5a$ for an integer a and then $xy = x(5a)$ and we see that 5 divides xy. □

Example 1.27. Suppose $n > 2$. If n is prime, then n is odd.

Proof. This seems obvious, but without the contrapositive it is not at all clear how to prove it directly. The contrapositive is, "for $n > 2$, if n is not odd then it is not prime" which is easy to prove. Indeed, if n is not odd then it is even and so 2 divides n, which shows it is not prime. □

1.3.3 Proof by Counterexample

Often times, mathematical statements will have the form $\forall x$: $P(x)$. If we want to disprove this statement, this means that we want to negate it:

$$\neg(\forall x : P(x)) \iff \exists x : \neg P(x)$$

and so it is sufficient to give a simple example of an x such that $P(x)$ does not hold. In formal proofwriting, however, it is not enough to merely supply an x for which $P(x)$ is non-truth; we must also justify why such an x is a valid counterexample, i.e. explain why $\neg P(x)$ is true.

Example 1.28. *Assess the truth of the equality*

$$\frac{1}{x+y} = \frac{1}{x} + \frac{1}{y}$$

for all $x, y \in \mathbb{R}$.

Proof. Choose $x = 2$, $y = 3$. Then

$$\frac{1}{2+3} = \frac{1}{5} \neq \frac{5}{6} = \frac{1}{2} + \frac{1}{3},$$

so the equality does not hold for all $x, y \in \mathbb{R}$. □

Example 1.29 (Euler)**.** Show whether or not it is true that for integers $n, k > 1$, if the sum of n many kth powers of positive integers is itself a kth power, then n is at least k; that is:

$$a_1^k + a_2^k + \ldots + a_n^k = b^k \implies n \geqslant k, \qquad a_i, n, k \in \mathbb{Z}$$

Proof. (Lander and Parkin, 1966.) It is false. Choose $(a_1, a_2, a_3, a_4, b) = (27, 84, 110, 113, 144)$, and check that

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

But $4 < 5$. ▫ □

Example 1.30. Determine whether $2^{2^n} + 1$ is prime for all integers $n \geqslant 0$.

Proof. (Euler) This is false. While $2^{2^n} + 1$ is prime for $0 \leqslant n \leqslant 4$, Euler showed that for $n = 5$, $2^{2^n} = 2^{32} + 1$ is composite. □