Lecture I: Proofs, Metric Spaces, Topology

Contents

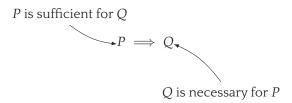
1	Proofs and Logic	1
2	Functions	3
3	Countability	3
4	Metric Spaces	5
5	Introduction to Topology	6
6	Limits	8

1. Proofs and Logic

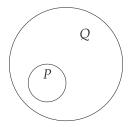
Math is a language: It should be possible to express anything you want in math, as you would in English or any another language. However, there are many things that are easier to express in math (just like many things are easier to express in English). One thing that is easier to do in math are proofs.

1.1. If *P* then *Q*. What does it mean?

• Logically, we say $P \implies Q$, that is, "P implies Q" or "P therefore Q."



• Graphically we say $P \subseteq Q$



Naturally, $P \implies Q \neq Q \implies P$; however we have that the *contrapositive* is equivalent, that is,

$$P \implies Q \equiv \neg Q \implies \neg P$$

This is to say, if not Q, then not P. Logically, if $P \implies Q$ and we do not have Q, then we cannot have P (otherwise we'd have Q). Graphically, if we are not in Q and $P \subseteq Q$, then we cannot be in P.

1.2. Proof Strategies.

1. **Direct**: Show $P \implies Q$. That is, find some path of logical statements that leads from P to Q.

Example 1. Show $m \in \mathbb{Z}$ even $\implies p \cdot m$ even $\forall p \in \mathbb{Z}$. If m is even, $\exists q \in \mathbb{Z}$ s.t. m = 2q, so pm = 2pq. Since $pq \in \mathbb{Z}$ we find pm is 2 times an integer, so it is even.

- 2. **Contrapositive**: If $\neg Q \Longrightarrow \neg P$. This is very similar to a direct proof, but often it is useful to rephrase a statement we want to prove in its contrapositive form. Further, texts will at times proceed by contrapositive without making explicit mention that is what they are doing.
- 3. **Contradiction**: If $\neg P$ leads to Q and Q is false, then P must be true.

Example 2. One of the most famous proofs by contradiction is that $\sqrt{2} \notin \mathbb{Q}$. Suppose the negation of that statement, that is, $\sqrt{2} \in \mathbb{Q}$. Recall

$$\mathbb{Q} = \{ p/q : p, q \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \}$$

That means that for some $p, q \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ that are co-primes we have that

$$\sqrt{2} = \frac{p}{q} \iff -2 = \frac{p^2}{q^2} \quad \text{or} \quad 2 = \frac{p^2}{q^2}$$

Note that if $\sqrt{2} = \widetilde{p}/\widetilde{q}$ where \widetilde{p} , \widetilde{q} are not co-primes, let m be the product of all the co-factors between them. Now define $p \equiv \widetilde{p}/m$ and $q \equiv \widetilde{q}/m$ to see that $\sqrt{2} = p/q$ for p, q co-primes. WLOG¹ let $2q^2 = p^2$:

$$2q^2 = p^2 \implies p^2 \text{ is even } \implies p \text{ is even } \implies \exists m \in \mathbb{Z} : p = 2m$$

Thus

$$2q^2 = (2m)^2 \iff q^2 = 2m^2 \implies q^2 \text{ is even } \implies q \text{ is even } \implies \exists n \in \mathbb{Z} : q = 2n$$

But that means that p, q are not co-primes (they have 2 as a common factor), a contradiction.

There is a very slight nuance with the proof above involving special cases. Can you spot it?²

- 4. *Induction*: We want to say something about statements that can be indexed by the natural numbers. Using induction we do that in two steps:
 - a) Prove the **base step**, P(1), is true.
 - b) Prove the *inductive step*, $P(k) \implies P(k+1)$, is true (i.e. assume P(k) is true and show P(k+1)).

¹WLOG means "Without Loss of Generality." This is occasionally used in proofs in order to shorten them: This means that even through there is more than one case to consider, proving any of them would follow identical steps to the one you are about to show; hence despite focusing on a specific case, the proof has not lost its general applicability (its generality).

²I believe the common definition of co-prime integers does not preclude both integers from being equal to 1, in which case my subsequent claims about p,q being even do not hold. If we wanted to be super careful we should say $p,q \neq 1$, but at the same time we can readily see that $1/1 \neq \sqrt{2}$.

Example 3. We want to show that the sum of the first k odd numbers is k^2 , that is:

$$\sum_{i=1}^{k} 2i - 1 = k^2$$

For the base case we can see $1 = 1^2$. For the inductive step, assume that P(k) is true show P(k+1):

$$\sum_{i=1}^{k+1} 2i - 1 = \sum_{i=1}^{k} 2i - 1 + (2k+1) \stackrel{!}{=} k^2 + (2k+1) = (k+1)^2$$

where $\stackrel{!}{=}$ is true by the inductive step assumption (if P(k) is true then $\sum_{i=1}^{k} 2i - 1 = k^2$).

2. Functions

We will not delve too much into set theory. Intuitively, however, we can think of a set as a collection of objects, and we can think of functions as rules that associate every element in one set with an element in another set.³

Definition 1. f is a *function* with *domain* X mapping to a *co-domain* Y if for every element $x \in X$ there exists a $y \in Y$ s.t. f(x) = y. We write $f: X \to Y$, and for any $S \subseteq X$

$$f(S) = \{ y \in Y : \exists x \in S \text{ s.t. } f(x) = y \}$$

is the *image* of S under f. f(X), the image of the domain, is called the *range*: The set of points in Y at least some element of X is mapped into.

Definition 2. If $f: X \to Y$ then for any $S \subseteq Y$ the *inverse image* of S is

$$f^{-1}(S) = \{ x \in X : \exists y \in S \text{ s.t. } f(x) = y \}$$

Remark 1. The inverse image is distinct from the concept of an inverse. A function is invertible if $\exists g$ s.t. $f(x) = y \iff g(y) = x$; this is also denoted $g = f^{-1}$ because the image of the inverse is the inverse image. However, functions needn't be invertible, while the inverse image is always defined.

In general it need not be the case that f(X) = Y, since some points of Y might not be mapped into. Further, a single point in Y might be the mapping of several points in X. We have some special interest in functions for which that is not the case.

Definition 3. A function $f: X \to Y$ is *injective* (or onto) if $f(x) = f(y) \implies x = y$.

Definition 4. f is *surjective* (or one-to-one) if f(X) = Y.

Definition 5. *f* is *bijective* or a bijection if it is injective and surjective.

3. Countability

Definition 6. A set X is *countably infinite* or *countable* if \exists a bijection from X to the natural numbers, \mathbb{N} .

³Formally, we can define a function f from X to Y as a binary relation s.t. $f \subseteq (X \times Y)$ and for each element $x \in X$ there is one (and only one) element $y \in Y$ s.t. $(x,y) \in f$ (though for each element in y there may be some $z \neq x$ s.t. $(z,y) \in f$). Chapter 1 of Ok has a rigorous treatment of functions following an introduction to set theory.

We make a distinction between finite and countable. Some examples of countably infinite sets:

- 1. \mathbb{N} is countable since a bijection from $\mathbb{N} \to \mathbb{N}$ is given by the identity f(x) = x.
- 2. \mathbb{Z} is countable. This is slightly more complicated, but we can enumerate all the integers:

$$\{0, -1, 1, -2, 2, \ldots\}$$

This is the enumeration given by the bijection f(x) = 2|x| - 1(x < 0)

Is \mathbb{Q} countable? Is \mathbb{R} ? The answers are yes and no, respectively, but the arguments are more nuanced.

Claim 1. \mathbb{Q} is countable.

Proof. Consider the function g(p,q) = p/q defined over $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. We can see that $\mathbb{Q} = g(\mathbb{Z} \times \mathbb{Z} \setminus \{0\})$. Hence $\mathbb{Q} \subset \mathbb{Z} \times \mathbb{Z}$, that is, the rational numbers are a subset of the Cartesian product of two countable sets. Since any sub-set of a countable set is countable, if $\mathbb{Z} \times \mathbb{Z}$ is countable the countability of \mathbb{Q} follows immediately. (The intuition is that when we construct the bijection, we can simply "skip over" the elements that are not in \mathbb{Q} , which in this case would be every alternative representation of a fraction.)

Take any P and Q countable; then we can enumerate their elements as

$$P = \{p_1, p_2, \ldots\}$$
 and $Q = \{q_1, q_2, \ldots\}$

And we can enumerate their Cartesian product as

$$Q \times P$$
 p_1 p_2 p_3 p_4 ... q_1 1 3 6 10 q_2 2 5 9 q_3 4 8 \ddots q_4 7 \ddots

meaning $P \times Q$ is countable. The bijection that corresponds to that table is

$$f(p_i, q_j) = \frac{(i+j-1)(i+j)}{2} - (i-1)$$

Claim 2. \mathbb{R} is not countable.

Cantor's Diagonal Argument. We proceed by contradiction.⁴ Suppose that \mathbb{R} is countable, so we can enumerate its elements as $\mathbb{R} = \{r_1, r_2, \ldots\}$. The decimal representation of each element in \mathbb{R} is then

$$r_1 = N_1.d_{11}d_{12}d_{13}...$$

 $r_2 = N_2.d_{21}d_{22}d_{23}...$
 $r_3 = N_3.d_{31}d_{32}d_{33}...$

⁴Cantor's diagonalization proof has been called one of the most beautiful proofs in mathematics.

:

where $N_i \in \mathbb{Z}$ and $x_{ij} \in \{0, ..., 9\}$. Take $y = N.y_1y_2y_3...$ s.t. $y_i \neq x_{ii}$ and y doesn't have an alternative representation (so y doesn't end in all 0s or all 9s; but we can do this, since for any x_{ii} we have 7 numbers to choose from other than 0, 9, or x_{ii}). $y \in \mathbb{R}$ but $y \neq r_i$ for all j, a contradiction.

Why doesn't this proof work for \mathbb{Q} ?⁵

4. Metric Spaces

Definition 7. A function $d: X \times X \to \mathbb{R}_+$ with $X \neq \emptyset$ is called a *distance* or a *metric* on X if

- 1. $d(x, y) = 0 \iff x = y$,
- 2. d(x, y) = d(y, x) (it is symmetric), and
- 3. $d(x, y) \le d(x, z) + d(z, y)$ (the triangle inequality holds).

Note that the triangle inequality says that you cannot "shorten" the distance between two points if you first "stop by" a third point. It might be equal (if z is in the path from x to y in some sense), but it can never be smaller. Last, note that we defined d to be ≥ 0 for all x, y.

Definition 8. A *metric space* (X, d) is a non-empty set X with a metric d defined on X.

Some examples of metric spaces:

1. For any $X \neq 0$, one way to metricize the space is the discrete metric

$$d(x,y) = \begin{cases} 1 & x \neq y \\ 0 & x = y \end{cases}$$

2. \mathbb{R}^N with the euclidean distance,

$$d(x,y) = ||x - y|| = \sqrt{\sum_{i=1}^{N} (x_i - y_i)^2}$$

3. More generally, consider the L^p norm, d_p , for $1 \le p \le \infty$ on \mathbb{R}^N for $N \in \mathbb{N}$

$$d_p(x,y) = \begin{cases} \left(\sum_{i=1}^N |x_i - y_i|^p\right)^{1/p} & 1 \le p < \infty \\ \max_{i=1,\dots,N} |x_i - y_i| & p = \infty \end{cases}$$

 (\mathbb{R}^N, d_p) is a metric space. d_2 is the euclidean distance, but it turns out that, while geometrically intuitive, it's not necessary to preserve a lot of the properties we care about.

⁵If we try to use that same proof to show $\mathbb Q$ is not countable there is actually no guarantee that the number y we construct will be an element of $\mathbb Q$. We have already established there are numbers that are not in $\mathbb Q$, whereas $\mathbb R$ is actually defined to be complete (this is a formal term, but intuitively it means that $\mathbb R$ has *all* the numbers).

 $\begin{array}{c|c} & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & \\ & & & \\ & &$

Figure 1: Unit "circle" in \mathbb{R}^2 under different L^p norms

In the figure above we can get some intuition for why we defined the d_{∞} norm as the max; graphically on \mathbb{R}^2 , we can see this is the natural extension of d_p as $p \to \infty$.

While it can be useful to developan abstract understanding of metric spaces, for the purposes of this class it's fine if you think of metric spaces as Euclidean space (i.e. (\mathbb{R}^N, d_2) , which I will simply denote as \mathbb{R}^N).

5. Introduction to Topology

Definition 9. Let X be a metric space. For each $x \in X$ we define the ε -neighborhood of x as

$$N_{\varepsilon,X}(x) = \{ y \in X : d(x,y) < \varepsilon \}$$

On \mathbb{R} , we can see this is just the interval of length 2ε centered around x; on \mathbb{R}^2 this is a circle, on \mathbb{R}^3 it is a ball, and so on. Neighborhoods are never empty, since at least $x \in N_{\varepsilon,X}(x)$.

Remark 2. In Euclidean space an ε -neighborhood is called an ε -ball. Henceforth we will use ε -balls in place of neighborhoods, denoting the ε -ball centered around a point x as $B_{\varepsilon}(x)$. However, the results we discuss will hold using the more abstract idea of a neighborhood in any metric space.

Definition 10. Let $S \subseteq \mathbb{R}^N$; S is **open** in \mathbb{R}^N if $\forall s \in S \ \exists \varepsilon > 0$ s.t. $B_{\varepsilon}(x) \subseteq S$.

Definition 11. Let $S \subseteq \mathbb{R}^N$; S is *closed* if its complement $S^C = \mathbb{R}^N \setminus S$ is open.

Some examples of open and closed sets:⁶

1. The interval (0,1) in \mathbb{R} is open. Take any 0 < x < 1 and let

$$\varepsilon \equiv \min\{x - 0.5(0+x), 0.5(1-x)\}$$

Note
$$N_{\varepsilon,\mathbb{R}}(x) = (x - \varepsilon, x + \varepsilon)$$
, so $0 < 0.5x \le x - \varepsilon < x < x + \varepsilon \le 0.5(1 + x) < 1$, means $N_{\varepsilon,\mathbb{R}}(x) \subseteq (0,1)$.

 $^{^6}$ Note the definition of openness uses ⊆ instead of ⊂. This can be an important distinction, and gets to the fact openness and closeness are not intrinsic properties of subsets: They are tied to the set they are defined in as well as the metric that has been defined on the space. Similarly, a set is defined as closed if its complement *in a given space* is open. All this might make you suspect that sets can be both open or closed if we simply change what they are open or closed relative to, and you would be right!

- 2. The interval [0,1] is closed in \mathbb{R} . $(-\infty,0)$ is open. For any x<0, take $\varepsilon=|x|/2$ and we have $-\infty< x-\varepsilon< x< x+\varepsilon<0$. Similarly, for x>1 take $\varepsilon=(x+1)/2$ and we get $1< x-\varepsilon< x< x+\varepsilon<\infty$. Since its complement is open, [0,1] is closed.
- 3. The interval [0,1) is open in \mathbb{R}_+ . This is a bit less obvious. [0,1) is not open in \mathbb{R} because if we take x=0, any $\varepsilon>0$ gives $x-\varepsilon<0$, and thus the ε -neighborhood is not in [0,1). However, in \mathbb{R}_+ there are no points <0, so there is nothing to contradict [0,1) being open.

What about [0,1) in \mathbb{R} ? Is it open or closed?⁷

Claim 3. The empty set \emptyset is both open and closed.

Proof. The complement of the empty set is $\mathbb{R}^N \setminus \emptyset = \mathbb{R}^N$, the space itself. Take any $x \in \mathbb{R}^N$ and any ε -ball $B_{\varepsilon}(x)$; by definition $B_{\varepsilon}(x) \subseteq \mathbb{R}^N$. Since \mathbb{R}^N is open, \emptyset is closed.

The empty set is open by vacuity: Pick $\varepsilon > 0$ and any $x \in \emptyset$; we have $B_{\varepsilon}(x) = \emptyset \subseteq \emptyset$. Another way to see it is the contrapositive: $\forall \varepsilon > 0$, if $B_{\varepsilon}(x) \not\subseteq \emptyset$ then $B_{\varepsilon}(x) \subseteq \mathbb{R}^N$, which implies $x \in \mathbb{R}^N$ and $x \notin \mathbb{R}^N \setminus \mathbb{R}^N = \emptyset$. (Note this also implies \mathbb{R}^N is closed.)

Can you prove that ε -balls are open?⁸

Definition 12. A set is "clopen" if it is both closed and open.

Claim 4. • Any union of open sets is open.

- A finite intersection of open sets is open.
- Any intersection of closed sets is closed.
- A finite union of closed sets is closed.

To see why we require a finite intersection for open sets, consider $I_n = (-1/n, 1/n)$ in \mathbb{R} . Each set is open, but $\bigcap_{n=1}^{\infty} I_n = \{0\}$, and singletons are closed in \mathbb{R} , so the infinite intersection is closed. Similarly, we can see why we need a finite union for closed sets: $\bigcup_{x \in (0,1)} \{x\} = (0,1)$; we just discussed how singletons are closed, but the infinite union can be open.

Definition 13. 1. The union of every open set O s.t. $O \subseteq S$ is the *interior* of S. We denote it as int(S).

- 2. The intersection of every closed set K s.t. $S \subseteq K$ is the *closure* of S. We denote it as cl(S).
- 3. The **boundary** of *S* is the set difference between the closure and the interior, $bd(S) = cl(S) \setminus int(S)$.

Claim 5. An open set is its own interior. A closed set is its own closure.

The interior is always open, since arbitrary unions of open sets are open; similarly, the closure is always closed, since arbitrary intersections of closed sets are closed.

Definition 14. Let $S \subseteq \mathbb{R}^N$; S is **bounded** if $\exists \varepsilon > 0, s \in S$ s.t. $S \subseteq B_{\varepsilon}(x)$.

Definition 15. Let $S \subseteq \mathbb{R}$; a is an *upper bound* for S if $\forall s \in S$ we have $s \leq a$. The least upper bound is called the *supremum*, denoted sup S.

⁷It's actually neither.

⁸Hint: You can use the triangle inequality.

 \Box

Definition 16. Let $S \subseteq \mathbb{R}$; b is an *lower bound* for S if $\forall s \in S$ we have $s \geq b$. The greatest lower bound is called the *infimum*, denoted inf S.

Claim 6. Let $S \subseteq \mathbb{R}$. $a = \sup S$ iff $\forall c < a \ \exists s \in S$ s.t. c < s; similarly, $b = \inf S$ iff $\forall c > b \ \exists s \in S$ s.t. c > s.

Proof. Let $a = \sup S$ and take any $c \in S$ s.t. c < a. By contradiction suppose $\forall s \in S$ we have $s \le c < a$, so c is an upper bound smaller than a, which contradicts the definition of the sup. Now let a be s.t. for any $c \in S$ with c < a there exists some $s \in S$ s.t. c < s. By contradiction, if $a \ne \sup S$ then by definition of the sup it must be that $\sup(S) < a$; however, by premise we now have $\exists s \in S$ s.t. $\sup S < s$, which contradicts the definition of the sup. Hence $a = \sup S$.

The arguments for the inf are entirely analogous.

Remark 3. For any $S \subseteq \mathbb{R}$ that is bounded above, $\sup S \in \mathbb{R}$; similarly, for any $S \subseteq \mathbb{R}$ that is bounded below, $\inf S \in \mathbb{R}$. This is not obvious as, for example, the set $\mathbb{Q} \cap (-\pi, \pi)$ does not have a \sup or an \inf in \mathbb{Q} . The fact this is true in \mathbb{R} is a consequence of a property called "completeness." We will not discuss it in depth in this class, but intuitively it means that \mathbb{R} has no "holes" (unlike, say, \mathbb{Q}). The real line \mathbb{R} is actually constructed to have this property, and you may encounter references to the *completeness axiom*.

Definition 17 (Archimedean Property). $\forall \varepsilon > 0 \ \exists N \in \mathbb{N} \text{ s.t. } 0 < 1/N < \varepsilon$.

Claim 7. \mathbb{Q} *is dense in* \mathbb{R} . *In this context,* $\forall a, b \in \mathbb{R}$ *s.t.* $a < b \exists q \in \mathbb{Q}$ *s.t.* a < q < b.

Proof. Density is defined as a more general property of metric spaces, but in the context of the real line the above is a good characterization: You can always find a rational number between any two real numbers. Since b-a>0, the Archimedean Property gives $\exists n\in\mathbb{N}$ s.t. 0<1/n<(b-a), or 1< n(b-a). Take any integer $m\in\mathbb{Z}$ s.t. na< m< nb (at least one such integer exists since the difference between na and nb is greater than 1). Since $n\in\mathbb{N}$ is strictly positive, dividing through preserves the inequalities, and

Let $q \equiv m/n \in \mathbb{Q}$ and we have completed the proof.

6. Limits

Definition 18. $s \in \mathbb{R}^N$ is a *limit point* of a set S if $\forall \varepsilon > 0$ there is some $x \in S$ s.t. $s \neq x$ and $d(s, x) < \varepsilon$.

Intuitively, it's any point in *S* that can be arbitrarily close to other points in *S*.

Definition 19. Let $f: S \to \mathbb{R}$ and s be a limit point of S. We say L is the *limit* of f(x) as x approaches s,

$$\lim_{x \to s} f(x) = L$$

if $\forall \varepsilon > 0 \ \exists \delta > 0$ s.t.

$$d(x,a) < \delta \implies |f(x) - L| < \varepsilon$$

Definition 20. Let $S \subseteq \mathbb{R}$, $f: S \to \mathbb{R}$, and s a limit point of S. The limit from above or from the right is

$$\lim_{x \to s^+} f(x) = L_+$$

if $\forall \varepsilon > 0 \ \exists \delta > 0 \text{ s.t.}$

$$s < x < s + \delta \implies |f(x) - L_+| < \varepsilon$$

Similarly for the limit from below (or from the left):

$$\lim_{x \to s^{-}} f(x) = L_{-}$$

We have that $\lim_{x\to s} f(x)$ exists if $L_+ = L_- = L$.

Keywords

ε -ball, 6 ε -neighborhood, 6 base step, 2 bijective, 3 boundary, 7 bounded, 7	image, 3 induction, 2 inductive step, 2 infimum, 8 injective, 3 interior, 7 inverse image, 3
clopen, 7 closed, 6 closure, 7 co-domain, 3 contradiction, 2 contrapositive, 2 countable, 3 countably infinite, 3	limit, 8 limit point, 8 lower bound, 8 metric, 5 metric space, 5 open, 6
dense, 8 direct, 2 distance, 5 domain, 3 function, 3	range, 3 supremum, 7 surjective, 3 upper bound, 7
idiletion, J	apper bound, /