Intro to Proofs

Juniper Bahr

October 2, 2021

Contents

1 Goals

In this document I'll introduce a lot of notation. Notation is

1. handy for being extremely precise

2. horrible if you have to read too much of it

Proofs are fundamentally *text designed for people*. Keep this in mind always when learning notation. Being super fancy and writing all sorts of cool symbols can be fun, but is less effective at conveying ideas. Always keep in mind that **proofs are written in sentences**.

English can be ambiguous about logic and this can trip a lot of people up sometimes. In English, "if it's raining out i've got an umbrella" is used to mean "I have an umbrella. It may be raining (in which case let's use it)". But mathematically/logically it means "If it's raining, I have an umbrella. If it's not raining, I may or may not have an umbrella" and would be a perfectly true thing to say when it's sunny and you don't have an umbrella. Logic and common usage of language don't always line up, and we need to be logically precise in mathematics.

The point of learning this compact notation is **not** to use it a lot, but to understand how we can logically construct clear mathematical sentences and learn how to be clearer when we write natural language (like English or whatever other language you're doing proofs in).

I'm hoping in this document to talk about

1. what sets are (and some basic operations)

2. what is a proposition

3. how do we prove basic types of propositions?

and throw in a few examples.

2 Sets

2.1 Basics

A set is one of the basic kinds of things we have in math, and much of mathmatics is ultimately built from it (unless you ask a logician).

A **set** is denoted with curly braces and the **elements** of the set are inside the curly braces, so $\{1, 2, 3\}$ is a set containing three numbers.

Sets ignore repetition and order, so $\{1,2,1\} = \{2,1\} = \{2,2,2,2,2,1\}$. These are all the same set.

We denote "is an element of" with the symbol $\in$ (that's `\in` in LaTeX).

2.2 Examples

- $\mathbb{N}$ is the set of natural numbers. Its elements are $1,2,3,\ldots$. Obviously I can't list them all. We might write something like $\mathbb{N} = \{1,2,3,4,\ldots\}$.
- $\mathbb{R}$ is the set of real numbers. I definitely can't list all of these. It includes positive numbers, negative numbers, rational numbers, irrational numbers, stuff like that. So $1, -4.2, \pi, -e$ are all individually members (another word for elements) of the set $\mathbb{R}$.
- $\mathbb{Z}$ is the set of integers. We have $\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$.

2.3 Subsets

Whenever we have two sets, A and B, and every element of A is *also* in B, we say that A is a **subset** of B and denote this $A \subseteq B$ (that's `\subseteq` in LaTeX). This $\subseteq$ symbol should remind you of $\leq$, because A is *contained in B* and could be equal to it.

Here, $\mathbb{N} \subseteq \mathbb{R}$ and $\{1\} \subseteq \mathbb{R}$, but $\{\{1\}\} \nsubseteq \mathbb{R}$ because the only element of $\{\{1\}\}$ is $\{1\}$ which is not an *element* of $\mathbb{R}$.

2.4 Equality

If $A \subseteq B$ and $B \subseteq A$ then every element of A is also in B, and every element of B is also in A. In other words, the two sets have the same elements. This is saying that the sets are equal!

So we write $A = B$ whenever $A \subseteq B$ and $B \subseteq A$.

2.5 Intersection and Empty Set

The intersection of two sets is everything in *both* of them. It is denoted $\cap$ (that's `\cap` in LaTeX).

So $\{1,2,3\} \cap \{3,4,5\} = \{3\}$.

What about the intersection of two sets that *don't overlap*? What is $\{1,2\} \cap \{3,4\}$?

Since *nothing* is in both of them, the intersection is $\{\}$, the **empty set**, which is also denoted $\varnothing$ (that's `\varnothing` in LaTeX from the package `amssymb`).

2.6 Unions

The union of two sets is everything in *either* of them. It's denoted $\cup$ (that's `\cup` in LaTeX).

So $\{1, 2, 3\} \cup \{3, 4, 5\} = \{1, 2, 3, 4, 5\}$.

2.7 Setminus

The difference of two sets is everything in one that's *not* in the other. It's denoted $\setminus$ (that's `\setminus` in LaTeX).

So $\{1, 2, 3\} \setminus \{3, 4, 5\} = \{1, 2\}$.

2.8 Set builder notation

Often we construct sets by saying "it's the set of (things) where (something about the thing is true)" like "the set of umbrellas that are green" or "the set of numbers that are even".

To do this, we use **set builder notation**:

$$\{x \in \mathbb{N} \mid x \text{ is even}\}$$

is an example.

The first portion is the *thing* and the second portion is *the property about that thing that defines membership*. There are better terms probably. We might write things like $A = \{2x \in \mathbb{N} \mid x \text{ is even}\}$. Then A is the set of "things of the form $2x$" such that "x is even". The | is often read as "such that".

Here $A = \{4, 8, 12, 16, \dots\}$ because it is the set of doubles of even numbers.

3 Propositions

3.1 Informal

A proposition is a statement that can be true or false, like "It's raining right now" or "There is an umbrella in my backpack".

More complicated things can be propositions too, like "If it's raining, then I have an umbrella in my backpack".

In math, we construct more complicated propositions from simpler ones.

3.2 Building up propositions

3.2.1 And

Whenever we have two propositions P and Q, we can form their "logical conjunction" $P \wedge Q$ (that's `\wedge` in LaTeX) which just means "both P and Q are true". You **should** just write P and Q which is simpler in basically every case.

3.2.2 Or

There's also a "logical disjuction" $P \vee Q$ (that's `\vee` in LaTeX) which just means "either P or Q".

$P \vee Q$ is true when

1. P is true and Q is false

2. P is false and Q is true

3. P is true and Q is true.

And when P and Q are *both* false, then $P \vee Q$ is also false.

It's easier to just write P or Q in basically every case, so that's greatly preferred.

3.2.3 Negation

We write $\neg P$ (that's `\neg` in LaTeX) to denote "not P". $\neg P$ is true whenever P is false, and vice versa.

3.2.4 Implication

We can write $P \implies Q$ (that's `\implies` in LaTeX) to mean "P implies Q". Specifically, $P \implies Q$ is true when

1. P is true and Q is true

2. P is false and Q is whatever

For example if "(it is raining) implies (i'm carrying my umbrella)" is true, then

1. whenever it's raining, I'm also carrying my umbrella

2. when it's not raining, i may or may not be carrying my umbrella.

It turns out that $P \implies Q$ is logically equivalent to $Q \vee (\neg P)$. Let's look at a truth table to see what happens in every case of P and Q being true or false.

P	Q	$P \implies Q$	$\neg P$	$Q \vee (\neg P)$
True	True	True	False	True
True	False	False	False	False
False	True	True	True	True
False	False	True	True	True

3.2.5 Biconditional

When $P \implies Q$ *and* $Q \implies P$, we write $P \iff Q$ (that's `\iff` in LaTeX). We will say "P is logically equivalent to Q" or "P holds iff Q holds" where "iff" is short for "if and only if".

3.3 Variables and quantifiers

3.3.1 Variables

Some propositions depend on a variable, like "n is even". If we call this proposition $P(n)$, then we can ask if $P(1)$ is true, or if $P(2)$ is true, etc.

We say in this instance "$P(2)$ holds" and "$P(1)$ fails" because 2 is even, but 1 is not.

3.3.2 Universal Quantifier

If $P(n)$ is *always* true (for n in some set A) we formally write "$\forall n \in A, P(n)$".

Usually this ends up like "$\forall n \in A$, $P(n)$ is true" or something like that.

$\forall$ is read as "for all" or "for every" and is `\forall` in LaTeX. It has the fancy name "universal quantifier".

3.3.3 Existential Quantifier

If $P(n)$ is true for *at least one* n in some set A we write "$\exists n \in A, P(n)$" or read "there exists an n in the set A where $P(n)$ is true".

$\exists$ is read as "there exists" or "for some" and is `\exists` in LaTeX. It has the fancy name "existential quantifier".

3.3.4 $\exists!$

Sometimes something is true for *just one* element in a set. When this holds, we write $\exists!\, n \in A, P(n)$ or read "there exists a unique $n \in A$ such that $P(n)$ holds".

$\exists!$ is read as "there exists a unique" or "there exists only one". It's `\exists !` in LaTeX.

3.4 Examples

Combining everything we know so far, try to express the following propositions in natural language. Then ask yourself if they're true or false.

1. $\forall x \in \mathbb{N}, \exists y \in \mathbb{R}, (x + y = 2) \lor (xy = 1)$
2. $\exists n \in \mathbb{R}, \forall m \in \mathbb{R}, m + n = 0.$
3. $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, m + n = 0.$
4. $\forall \varepsilon > 0, \exists \delta > 0, (\delta < \varepsilon^2)$

Do you find it's easier to understand what's going on in natural language or mathematical notation?

4 Proofs

4.1 Basics

Proofs are a form of technical writing. The primary goal of a proof is to *convince a person.* While I've shown you lots of symbols in this document, it's important that **a proof is not a giant list of symbols.**

While it's good to have notation to compactly represent things, it's **really hard to read!**

Which is easier to read:

1. $\forall a \in \mathbb{R}, \forall \varepsilon \in \{x \in \mathbb{R} \mid x > 0\}, \exists \delta \in \{x \in \mathbb{R} \mid x > 0\}, \forall b \in \mathbb{R}, |a - b| < \delta \implies |f(a) - f(b)| < \varepsilon.$
2. f is continuous.

The second one is much easier.

When you can express things in words easily, do so!

4.2 How do we prove things?

The following sections talk about how to prove different kinds of statements, then we'll see them put together in a few different ways.

4.3 And, Or, Not, Implies

4.3.1 And

In order to prove $P \wedge Q$, prove that P is true **and** that Q is true.

Do them one at a time.

4.3.2 Or

In order to prove $P \vee Q$, show that at least one of P and Q must be true.

This can be done directly or in a few different ways.

You can assume P is false and show that Q has to be true. Or you can show that when Q is false, P has to be true.

Sometimes it's easier to show that "both P and Q are false" *isn't true*.

4.3.3 Not

To show $\neg P$ is true, show that P is false. And vice-versa.

This probably sounds silly, but negating more complicated logical statements can be tough without practice.

4.4 How to negate (and simplify propositions)

If we want to show that P is false, we need to show that $\neg P$ is true. But what if P is very complicated? We work left to right to negate a complicated expression with the following rules:

1. $\neg(\forall x, P(x))$ is equivalent to $\exists x, \neg P(x)$

2. $\neg(\exists x, P(x))$ is equivalent to $\forall x, \neg P(x)$

If it's *false* that every x satisfies $P(x)$, then there is an x where $P(x)$ is false. And if it's *false* that there exists an x such that $P(x)$ holds, then for every x, $P(x)$ must fail to hold.

We also use *de Morgan's Laws*

1. $\neg(P \vee Q) \iff (\neg P) \wedge (\neg Q)$. If not (either P or Q is true) then neither P nor Q can be true!

2. $\neg(P \wedge Q) \iff (\neg P) \vee (\neg Q)$. If it's false that they both hold, then one or the other must fail.

4.5 Converse, Inverses, Contrapositives, Oh My

1. The *contrapositive* of a statement in the form $P \implies Q$ is the proposition $\neg Q \implies \neg P$. It is logically equivalent to the original statement, so whenever you see $P \implies Q$, you know you can replace it with $\neg Q \implies \neg P$ if you want to.

2. The *converse* of $P \implies Q$ is $Q \implies P$. It is **not** logically equivalent to $P \implies Q$. So you can have $Q \implies P$ *true* while $P \implies Q$ is *false*! Swapping an implication for a converse is an *easy and common mistake*! Be careful.

3. The inverse of $P \implies Q$ is $\neg P \implies \neg Q$. It is **not** logically equivalent to $P \implies Q$, but the inverse *is* the contrapositive of the converse, so the *inverse and converse are logically equivalent to each other.*

4.6 Quantifiers

4.6.1 Proving a $\forall$ statement

If you want to prove $\forall x \in A, P(x)$, your proof will look like:

> Let $x \in A$.
>
> Since x is in A and A is defined as (something), we know that x satisfies (something).
>
> (some more arguments here)
>
> Thus we see that $P(x)$ holds true.
>
> Since we showed $P(x)$ holds for an arbitrary $x \in A$, we have $\forall x \in A, P(x)$ as desired.

Sometimes it may be easier instead to show that $\neg(\forall x \in A, P(x))$ is *false*. Remember that this simplifies to showing that $\exists x \in A, \neg P(x)$ is false. To show this is false, we can assume there *is* an $x \in A$ satisfying $\neg P(x)$ and find a *contradiction.* I'll clarify this in a *proof by contradiction* section.

4.6.2 Proving an $\exists$ statement

If you want to prove $\exists x \in A, P(x)$, your proof will look like:

> We want to show that there exists an $x \in A$ such that $P(x)$ is true.

(in your scratch work, try to find an example of such an x. if you can't, consider showing why if no such x exists, there's a contradiction, i.e., assume no x exists such that $P(x)$ is true and conclude something impossible, like $1 = 0$. This will tell you that there *must* be an x. Normally finding an x directly isn't too bad.)

Consider $x =$ (whatever you figured out from your scratch work)

We want to show that $x \in A$ and that $P(x)$ is true.

(argument goes here)

Thus $x \in A$ and $P(x)$.

Since we found an example of an $x \in A$ where $P(x)$ holds, we see that $\exists x \in A, P(x)$ is true.

4.7 Subsets, Equality, Double Containment

4.7.1 Proving $A \subseteq B$.

Remember that $A \subseteq B$ whenever $x \in A$ implies $x \in B$, or phrased with a quantifier: $\forall x \in A, x \in B$.

We can now prove this like we'd prove any $\forall$ statement. The proof will open up:

"Let $x \in A$"

and then we will usually "unpack" what being in A means (for instance, if A is the set of even numbers, then we can write $x = 2k$ for some $k \in \mathbb{Z}$).

Eventually we will deduce that $x \in B$, and our proof will end with

"thus $x \in B$. And since the above held for any $x \in A$ we see that $\forall x \in A, x \in B$. Thus $A \subseteq B$.

4.7.2 Proving $A = B$.

What if you want to show that two sets are equal? The standard way is to show *double containment*.

Recall that $A = B$ if and only if $A \subseteq B$ *and* $B \subseteq A$. So to prove $A = B$, just prove both $A \subseteq B$ and $B \subseteq A$!

Warning: it's a common mistake to try to show $A = B$ by "massaging" the definition of the set A into the set B. For instance, if I want to show

$$\{x \in \mathbb{N} \mid \exists k \in \mathbb{Z}, x = 2k\} = \{y \in \mathbb{N} \mid \exists k, \ell \in \mathbb{Z}, y = 4k \text{ or } y = 2(2\ell + 1)\}$$

a common error is to start by messing with those conditions in the above definitions of the sets. Like *beginning* by writing things about k and ℓ and trying to compare them to the k in the definition of the first set.

This really leads to a logical mess very fast, and the only thing this promises to make faster is not having to show a double containment. Don't be tempted! Just do the double containment proof. It's much less messy and confusing in my opinion. And more convincing.

4.8 Proof Techniques and Types

4.8.1 Proof by contradiction

Let's say I want to show that 3 is odd and I'm having a tough time. Sometimes it helps to assume that what you're trying to show is *false* and show that *absolute nonsense follows*.

In other words, if I *assume 3 is even*, I can say $3 = 2k$ for some $k \in \mathbb{Z}$, and so $k = 3/2$ is an integer. But $3/2$ is a rational number and not an integer! So "3/2 is an integer" is both true *and* false! This is horrible! Nothing can be true and false at the same time!

Since I assumed something and concluded a contradiction, it *must* be that 3 is **not** even.

More formally, instead of showing P, show that assuming $\neg P$ results in a contradiction.

4.8.2 Direct Proof

This is often talked about in contrast to proof by contradiction. Here when you want to show $P \implies Q$, a "direct proof" is one where you just assume P and then show that Q holds true.

It's not much of a proof technique but the term does come up.

4.8.3 Constructive vs. Nonconstructive proofs

In order to show $\exists x, P(x)$, sometimes you can directly produce an x that *witnesses* the truth of $P(x)$ (by which I mean $P(x)$ is true for that particular x). These proofs are typically called *constructive* proofs.

Other times, you can show $\exists x, P(x)$ without saying exactly what x is. This can come up in a proof by contradiction, for example. When we don't know anything about the x that makes $\exists x, P(x)$ true, it is a *non-constructive* proof.

These aren't techniques so much as descriptors.

4.8.4 Induction

Induction is a very powerful proof technique that let's you show lots of things.

If you want to show $\forall n \in \mathbb{N}, P(n)$, you can

1. assume n is a natural number and somehow show that $P(n)$ is true
2. do something weird with a proof by contradiction maybe?
3. induction!

Induction is the reliance on the following fact:

> If $P(1)$ is true and $\forall n \in \mathbb{N}, P(n) \implies P(n+1)$, then it's true that $\forall n \in \mathbb{N}, P(n)$.

Think of a chain of dominoes. If I can guarantee that

1. The first domino falls down
2. Whenever the nth domino falls, the next one is sure to fall down too

Then *by induction*, I have shown that every domino falls.

As a simple example, let's show that n^3+2n is divisble by 3 for every n. Note that I wrote "for every n" at the end for convenient english even though this translates to the formal expression $\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, n^3+2n = 3m$.

Showing this directly seems tough, so let's see if we can do it with induction.

Proof. Let's show n^3+2n is divisible by 3 for every n by induction. Let $P(n)$ represent the proposition "n^3+2n is divisible by 3".

First we show the **base case**, $P(1)$. Since $1^3+2(1)=3$ and 3 is divisible by 3, we see that the base case holds true.

Next we must show that $P(n) \implies P(n+1)$ for any n. To do this we will **assume** that for **some** n, we have $P(n)$. We will try to conclude that $P(n+1)$ also holds.

(Be careful here! It is a common mistake to instead assume that $P(n)$ holds for **every** n but this is the *entire thing we wanted to show* We can't show something by assuming it first!)

Assume there is $n \in \mathbb{N}$ such that $P(n)$ holds. Then n^3+2n is divisible by 3, that is, there exists k such that $n^3+2n = 3k$.

We'd like to show that $P(n+1)$ holds, i.e., $(n+1)^3+2(n+1)$ is divisible by

3. We calculate

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 3n + 1 + 2n + 2 \\ &= n^3 + 2n + 3(n^2 + n + 1) \\ &= 3k + 3(n^2 + n + 1) \\ &= 3(n^2 + n + 1 + k),\end{aligned}$$

where most steps are algebraic simplification and a substitution of $n^3 + 2n$ for $3k$.

(Note: it's best if you have lots of lines to stop the long chain of equations to explain what's going on! It's really hard to follow much of this unless they're all very simple steps. Err on the side of explaining too much!)

Then for $h = n^2 + n + 1 + k$, an integer, we see that $(n+1)^3 + 2(n+1) = 3h$. This means that $(n+1)^3 + 2(n+1)$ is divisible by 3, and so $P(n+1)$ holds.

Thus we've shown that $P(n) \implies P(n+1)$.

Since $P(1)$ holds, and whenever $P(n)$ holds, we see that $P(n+1)$ also holds, we conclude *induction*, that $\forall n \in \mathbb{N}, P(n)$ holds. In other words, for every natural number n, we have that $n^3 + 2n$ is divisible by 3. □

4.9 Examples

4.9.1 Example 1

Let's prove that $\forall n \in \mathbb{N}, \exists x \in \mathbb{R}, n + 2x = 0$.

Proof. We will show $\forall n \in \mathbb{N}, \exists x \in \mathbb{R}, n + 2x = 0$.

First, let $n \in \mathbb{N}$. We would like to find an $x \in \mathbb{R}$ now such that $n + 2x = 0$.

(scratch work that I wouldn't include in the final proof: if $n + 2x = 0$, then $n = -2x$, so $x = -n/2$ should be our choice)

Consider $x = -n/2$. This is a real number since $\mathbb{N} \subseteq \mathbb{R}$ and the reals are closed under multiplication and division.

We'd like to show that $n + 2x = 0$. We calculate as follows:

$$\begin{aligned}n + 2x &= n + 2(-n/2) \\ &= n - n \\ &= 0\end{aligned}$$

Since $x \in \mathbb{R}$ satisfies $n + 2x = 0$, we see that $\exists x \in \mathbb{R}, n + 2x = 0$ is true.

As this holds for any $n \in \mathbb{N}$, we've shown the result: $\forall n \in \mathbb{N}, \exists x \in \mathbb{R}, n+2x = 0$. □

It's important to note that this scratch work doesn't fit the flow of the proof and isn't logically connected. Don't include it, but *do* do it.

4.9.2 Example 2

Let's show that the product of an even and an odd number is even.

The set of even numbers is $\{2n \mid n \in \mathbb{Z}\}$ or equivalently $\{m \mid \exists k \in \mathbb{Z}, m = 2k\}$

The set of odd numbers if $\{2n+1 \mid n \in \mathbb{Z}\}$ or equivalently $\{m \mid \exists k \in \mathbb{Z}, m = 2k+1\}$.

Let's use the second definition of both.

Proof. Let a be odd and b be even. This means there exists $n \in \mathbb{Z}$ such that $a = 2n$ and there is some $k \in \mathbb{Z}$ such that $b = 2k+1$.

(Note that we can't write $a = 2n$ and $b = 2n+1$! We need to pick different variable names here!)

We'd like to show that ab is even. We calculate

$$ab = 2n(2k+1) = 2(2nk+n)$$

Set $h = 2nk + n$. This is an integer since 2, n, and k are, and integers are closed under addition and multiplication. Since $ab = 2h$ with h an integer, we see that ab is even.

Thus the product of any even number with any odd number is even. □

4.9.3 Example 3

Let's show that the sum of two odd numbers is even using the definitions from above.

Proof. Let a, b be odd numbers. Then there exists $n, m \in \mathbb{Z}$ such that $a = 2n+1$ and $b = 2m+1$.

We'd like to show that the sum $a+b$ is even. We calculate

$$a + b = 2n + 1 + 2m + 1 = 2(n + m + 1)$$

Writing $k = m + n + 1$ which is an integer, we see that $a + b = 2k$, so $a + b$ is even.

Thus the sum of any two odd numbers is even. □

4.9.4 End of examples discussion

You may notice in here that when I have a proposition like $\forall x \exists y \forall z \exists w \ldots P$ the proof is basically guaranteed to look like this:

> Let x be (somewhere). Let's find a y.
>
> (scratch work)
>
> Consider $y =$ (something).
>
> Let z be (somewhere). Now let's find a w.
>
> (scratch work).
>
> Set $w =$ (something).

$\vdots$

> Let's now show that P is true.
>
> (more work)
>
> Thus P holds.

$\vdots$

> Since we found such a w we see that $\exists w \ldots P$
>
> And since this holds for any z, we have $\forall z \exists w \ldots P$
>
> We found such a y and so $\exists y \forall z \exists w \ldots P$
>
> And finally, this holds for any x, so we have $\forall x \exists y \forall z \exists w \ldots P$.

If you'd like to think of it this way, every quantifier on the left introduces a *layer* around the proof. The $\forall$ quantifier means you start your proof with "let" and end it with "which holds for every…". The $\exists$ quantifier means you start your proof with "Consider x =" and end it with "Which holds for the x we found, so $\exists x, \ldots$" is true.