Lecture Notes For: Mathematical Proof

Ali Fele Paranj
alifele@student.ubc.ca

February 23, 2023

This lecture note contains the material in the course MATH 220 Mathematical Proof (UBC 2023). However have exapnded the material and examples using the following books:

- Main Teextbook: PLP (an introduction to mathematical proof). Link: PLP website
- Book of Proof (3rd Edition) By Richard Hammack.
- Mathematical Proofs: A Transition to Advanced Mathematics By Chartrand et. al.
- Math proof lectures on YouTube: YouTube Link

Also some useful information can be found here which are the course content of this course in previous years.

- https://personal.math.ubc.ca/~ilaba/teaching/math220_F2015/
- https://secure.math.ubc.ca/php/MathNet/courseinfo.php?session=2020W&t=outline&name=220:101

Some open text books also can be found here in this link: https://aimath.org/textbooks/approved-textbooks/

Also I will add some material from the book "A first course in logic" by Hedman.

1 A little Bit Logic and Some Definitions

Symbolic logic and mathematical proof are tightly coupled to each other and can even be thought of a same thing. That's why in my opinion, doing mathematical proof requires two things: being familiar with mathematical logic(symbolic logic) and writing the ideas cleanly. Here in this section we will practice the first factor (logic) and the second one will be practiced throughout this text.

1.1 Basic Logic Operations

First of all we start with the definition of statement.

Definition: statement

An statement is a sentence to which a certain truth value can be assigned. So a mathematical statement should be True or False (can not be both at the same time and can not be non of them (the law of excluded middle)).

For example followings are some true statements:

- It is raining
- Aristotle is dead
- 2 is equal to 4

However some sentences (for example the self referencing sentences) can not be though of as statements since we can not assign a truth value to them. If we try to assign any truth value then we will have contradiction. For example:

- This sentence is False.
- The set of all sets that do not contains themselves, contain itself. We can state this in a mathematical wording: Let $A = \{X | X \notin X\}$ then $A \in A$.

It is very likely to come up with some sentences that their truth value depends on the value of a specific variable in the sentence. For example "x is an even number". We call these sentences as the **open sentences**.

You might agree that the statemented are not very interesting by their own. They do not have any dynamics. There are not any ways (at least so far) to combine them and generate new statements (with a certain truth value). Logic operators will do this for us. Logic operators are operators that can combine statements and produce new statements. It turns out that all of the logic operators can be boiled down to just two logic operators: NOT and AND.

1.1.1 NOT Operator

The act of a null operator on a statement will toggle its truth value. So NOT(True) will be false and NOT(False) will be True. Given this property of the NOT operator we can define it using its truth table

Definition: Not Operator

NOT operator: NOT operator toggles the truth value of an statement and has the following truth table

P	$\neg P$
0	1
1	0

The following statements are some examples of the act of the NOT operator:

- $\neg$(2 is even) is (2 is odd)
- $\neg$(Aristotle is dead) is Aristotle is alive

1.1.2 AND Operator

AND operator (with symbol $\wedge$) is a way to combine two statements and the truth value of the composite statement will be true only when both sub statements are true. So we can define the AND operator as following:

Definition: AND Operator

AND operator ($\wedge$) combines two statements P, Q in the following way:

P	Q	$P \wedge Q$
1	0	0
1	1	1
0	0	0
0	1	0

For example we can combine the following statements with AND operator and determine the truth value of the combined statement

- (Aristotle is dead (True)) $\wedge$ (Aristotle was a man (True)) : True Statement
- (4 is a prime number (False)) $\wedge$ (16 is an even number (False)): False Statement
- (That cat is alive) $\wedge$ (That cat is dead): False Statement (regardless of the truth value of the statements)

1.1.3 OR, Implication, and Bi conditional Implication

The operators AND and NOT are enough to express any kind of statements using the atomic statements. What I mean is that defining the AND and NOT operators for a computer is enough to parse and express any logical statements. However, to increase the readability for humans, we also define other logical operators based on the AND and NOT operators.

OR Operator: OR is an important logical operator that we use in our everyday life very frequently. If we combine two statements (sub-statement) with OR operator then the resulting statement is always true unless the two sub-statements are false.

Definition: OR Operator

OR Operator: The OR operator (denoted by the symbol $\vee$) is defined as

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

Using the RHS of the equation above we can calculate the truth table of OR operator as the following

P	Q	$P \vee Q$
1	0	1
1	1	1
0	0	0
0	1	1

Implication: Implication is one the most important logic operators that we will be using extensively in mathematical proof. The implication is not symmetric (unlike the AND and OR operators that were symmetric) the order is important. The following box defines implications and its truth table.

Definition: Implication

Implication: The implications operator (denotes with the $\Rightarrow$ or $\rightarrow$) is defined as:

$$P \Rightarrow Q \equiv \neg P \vee Q$$

In which P is called the *hypothesis* or *antecedent* and Q is called the *conclusion* or *consequent* and statement is read as is read as:

P implies Q
If P then Q

The truth table of the implication can be calculated using the RHS of its definition.

P	Q	$P \Rightarrow Q$
1	0	0
1	1	1
0	0	1
0	1	1

The second and the third rows of the truth table has its own names which are "affirming the antecedent" and "denying the consequent" correspondingly.

The first and the second row the the truth table of the implication operator seems reasonable. However the third and the forth rows look quite bizarre considering our daily experiences of using implication. For example, similar to the forth row we can write:

If Tabriz is in Europe, then Tehran is in Africa

Although this might make sense (a little bit!) but we rarely use this kind of implication in our everyday life. Because of the bizarreness of these cases, we actually have a different names for them in symbolic logic.

Vacuously True: If the hypothesis of an implication is false, then the implication is true no matter what is the truth value of its conclusion. In this case we say that the implication is vacuously true (the 3rd and 4th rows of the truth table of the implication).

Trivially True: If the conclusion of an implication is true, then the implication is always true, no matter what is the truth value of the hypothesis. In this situation, we call the statement to be trivially true (the 2nd and 4th rows of the truth table of the implication).

Modus Ponens: By analyzing the truth table of the implication we can observe that if the implication is true, then there is only one case the the antecedent is true and the consequent is also true. So if we know an implication is true, then by knowing the truth of hypothesis, we can infer the truth of the conclusion. This is called **Modus Ponens** or *affirming the antecedent*.

Modus Tollens: Modus Tollens is quite opposite of the modus ponens. By looking at the truth table of the implication we can see that if the implication is true and the consequent is false, then the antecedent should also be false. So if we know that the implication is true, and the conclusion is false, then we can conclude that the hypothesis is false as well. This kind of inference is called **Modus Tollens** or *denying the consequent*

Operations on the Implication: Since the implication is polar (the order matters), then we can perform different kind of operations on it which are summarized as the following.

Definition: Contrapositive, Converse, Inverse

Consider the implication

$$P \Rightarrow Q$$

Then we can define:

Contrapositive:

$$\neg Q \Rightarrow \neg P$$

Converse:

$$Q \Rightarrow P$$

Inverse:

$$\neg P \Rightarrow \neg Q$$

It is easy to show that the contrapositive of an implication has the same truth value as the implication. Also, we can show that these three operations are connected to each other in a circular way. i.e.

Contrapositive of Converse: Inverse
Converse of Inverse: Contrapositive
Inverse of Contrapositive: Converse

Chaining the Implications: Often in the mathematical proof, we chain the implications to each other (smaller steps) to prove a bigger implication. This is possible since the following statement is a tautology (it is always true)

$$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$$

By looking at the truth table of the RHS and LHS we can observe that those have same truth values.

P	Q	R	$P \Rightarrow Q$	$Q \Rightarrow R$	LHS	RHS	LHS $\Rightarrow$ RHS
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

We can use the induction to show that we can link multiple implications as the following:

$$((P \Rightarrow P_1) \wedge (P_1 \Rightarrow P_2) \wedge \cdots \wedge (P_n \Rightarrow Q)) \Rightarrow (P \Rightarrow Q) \tag{1.1}$$

Bi Conditional Implication: The bi conditional implication is true when an implication and its converse is true at the same time.

Definition: BiConditional Implication

The biconditional (represented with the symbol $\Leftrightarrow$) is defined as:

$$P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

and is read as:

P if and only if Q
P iff Q
P is necessary and sufficient condition for Q

The truth table of the biconditional is as the following

P	Q	$P \Leftrightarrow Q$
0	0	1
0	1	0
1	0	0
0	1	1

1.2 Axiom, Theorem, Corollary, Lemma, and Proposition

In this section we will review some basic definitions in the mathematical proof and mathematical logic.

Definition: Axiom

Axiom is a mathematical statement whose truth is accepted without proof.

For example the followings are some well-known axioms in mathematics:

- Kolmogorov axioms (axioms of probability)
- Axioms of the Euclidean geometry: For every line l and point P that is not on the line, there exists only one line l' that contains the point P and is parallel to the line l.

Definition: Theorem

A true mathematical statement whose truth can be verified using mathematical proof and following mathematical proof.

However, the mathematicians reserve the word theorem for true mathematical statements that is significant and very important. For instance the fact that $2+3=5$ is a true mathematical statement whose truth can be verified using mathematical proof. However, since it is not a significant results, it is not common to call it a theorem. Instead, alternative words are used like: proposition, results, fact, observation.

2 Direct Proof

It is often the case in the mathematical proof that we start with assuming the hypothesis of an implication is true and conclude with the truth of the conclusion of the implication. The general structure of those proves will be all similar. Suppose that we want to prove that the implication

$$P \Rightarrow Q$$

is true. When know that if P is false, then the statement will automatically be true. But if P is true, then the implication will be true only when the Q is true. So if we start by assuming that P is true and *through linking smaller true implications* we arrive at the conclusion, then by using modus ponens we can infer that conclusion of the original implication is also true. In other words, to prove $P \Rightarrow Q$ is true, we need to construct the following **true** implications:

$$\begin{aligned} P \Rightarrow P_1 &\quad \text{is true} \\ P_1 \Rightarrow P_2 &\quad \text{is true} \\ P_2 \Rightarrow P_3 &\quad \text{is true} \\ &\vdots \\ P_n \Rightarrow Q &\quad \text{is true} \end{aligned}$$

Then we can connect these statements with AND operator and have:

$$(P \Rightarrow P_1) \wedge (P_1 \Rightarrow P_2) \wedge \cdots \wedge (P_n \Rightarrow Q)) \Rightarrow (P \Rightarrow Q) \tag{2.1}$$

Here at this point there are two ways to proceed with the proof. In the following section I'll discuss both of them:

The first method to proceed with the proof: In this point of view, we assume that the statement P is true. Since the first baby implication is also true, then using Modus Ponens we can infer that P_1 is also true. Then since P_1 is true and the second baby implication is also true, then using Modus Ponens we can infer that P_2 is also true. Using the same logic we can infer that $P_3, P_4, \cdots P_n$ are also true. And for the last time, since the last baby statement is true and P_n is also true, then we can infer (using Modus Ponens) Q is also true. So we started with the true hypothesis and we arrived at the true conclusion. So utilizing the truth table of implication we can infer that the implication $P \Rightarrow Q$ is true.

The second method to proceed with the proof: The golden equation in utilizing this method is 2.1. From now on, when I mention RHS and LHS, I mean the right hand side and the left hand side of the equation 2.1. Since all of the statements in the LHS is true, then the whole statement in the LHS is also true. And since the statement LHS $\Rightarrow$ RHS is also true (check out the equation 1.1), then we can infer (modus ponens) that the LHS of the implication (i.e. $P \Rightarrow Q$) is also true. So if P is true then Q is also true.

These two methods are not really two different methods. These are two different methods to think about the same thing are are actually two sides of a single coin!

Example: Is n^2 Even or Odd?

Question. Let n be an integer. prove that if n is even, then n^2 is also even.

Scratch Paper Stuff. We are going to use direct proof method. So let's construct the first baby implication. let the statement P be:

P: integer n is even

and let the statement P_1 be:

$$P_1\text{: n can be written as } n = 2k, k \in \mathbb{Z}$$

From the definition of even numbers we know that the implication $P \Rightarrow P_1$ is true. Now lets construct the second baby implication. Let the statement P_2 be:

$$P_2\text{: the square root of } 2k \text{ is } 4k^2$$

From the properties of the multiplication of integers we know that if $a = b$ then $ac = bc$ for any integer c and the since the $a = b = c = 2$ is an special case of this property, then $P_1 \Rightarrow P_2$ is also true. Let's construct the third baby implication. Let the statement P_3 be:

$$P_3\text{: the integer } 4k^2 \text{ can be written as } 2(2k^2)$$

Considering the associativity property of the multiplication (i.e. $(ab)c = a(bc)$) then we know that the statement $P_2 \Rightarrow P_3$ is also true. And finally, we can utilize the definition of the even number once again and construct the following final baby implication step. Let Q be the statement

$$Q : n = 2(2k^2) \text{ is an even number}$$

Because of the definition of the even number we know that $P_3 \Rightarrow P_4$ is also true. So in a nutshell we have:

$$\begin{aligned} P &\Rightarrow P_1 \text{ is true (definition of even number)} \\ P_1 &\Rightarrow P_2 \text{ is true (property of integers)} \\ P_2 &\Rightarrow P_3 \text{ is true (associativity property of integers)} \\ P_4 &\Rightarrow Q \text{ is true (definition of even number)} \end{aligned}$$

By connecting these statements to each other with AND operator, we can write:

$$((P \Rightarrow P_1) \wedge (P_1 \Rightarrow P_2) \wedge (P_2 \Rightarrow P_3) \wedge (P_4 \Rightarrow Q)) \Rightarrow (P \Rightarrow Q)$$

Since all of the terms on the LHS is true, and the whole statement is also true (proved in 1.1) we can infer (modus ponens) that the right hand side is also true. We need a little extra step here to complete the proof: Since the statement P is true, and the statement $P \Rightarrow Q$ is also true, then we can infer (Modus Ponens) that Q is also true. □

Clean Proof. Assume $n \in \mathbb{Z}$ is even. Using the definition of even numbers, we can write n as $n = 2k$ for some integer k. Now squaring the both sides of the equation and factoring 4 we can write: $n^2 = 4k^2 = 2(2k^2)$. Since $2k^2 \in \mathbb{Z}$, it follows from the definition that n^2 is even. □

You might be wondering what is the square block (i.e. □) at the end of each proof. This is called "QED" which stands for "quod erat demonstrandum" which means " which was to be demonstrated". There are also other symbols in common use for this purpose that ♦, ■ are the most common alternatives.

2.1 Proof of Inequalities

Although there are not such a thing as a general recipe for mathematical proof. But we can add some kind of tricks to our tool kit. Here in this section I will describe one of them that might come very handy in dealing with inequalities. To better demonstrate the idea, I would like to proceed with an example.

Example: Tricks in Working with Inequalities

Question. Let $x, y \in \mathbb{R}$. Then prove $x^2 + y^2 \geq 2xy$

Scratch Paper Proof. When dealing with inequalities, it is better by studying a difference derived from the inequality. Let's start with studying the expression $x^2 + y^2 - 2xy$. As soon as we start dealing with this, we observe that we can write it as $(x - y)^2$. Since $x - y \in \mathbb{R}$ then we know that $(x - y)^2 > 0$. So we got the intuition that if we start with the difference of real numbers x, y, we can square it and then utilize the fact that the square should be positive and then arrive at the conclusion. Let's put these insights into good words and have more cleaner version of proof that has the appropriate flow of logic. □

Proof. Let x, y be real numbers. Hence $(x - y) \in \mathbb{R}$ and we can write $(x - y)^2 \geq 0$. Expanding this will give: $(x - y)^2 = x^2 + y^2 - 2xy \geq 0$. This can be rewritten as: $x^2 + y^2 \geq 2xy$. □

So the trick in a nutshell is: To prove and inequality, start with studying a difference (maybe the RHS-LHS). This trick is far from being a general recipe for mathematical proof. There any MANY MANY MANY occasions that this will not work at all. So do not over use any trick in your toolbox.

Example: Multiplying Inequalities

Question. Let $a, b, c, d \in \mathbb{R}$ and $a > b > 0$ and $c > d > 0$. Prove $ac > bd$.

Proof. Since $c > 0$ and $b > 0$ then we can multiply c at the first inequality and b at the second inequality without changing the direction of the inequality sign. So we will have:

$$ac > bc > 0$$
$$bc > bd > 0$$

So by combining these two inequalities, we can have:

$$ac > bd$$

Scratch Paper Proof. There is a reason that I am writing the scratch paper proof after the main proof. That is to show that how this kind of proof matches with the logical baby steps. Let the statements P_1, P_2 be defined as:

$$P_1 : a > b > 0$$
$$P_2 : c > d > 0$$

Let's define the statements P as an auxiliary statement in the following way:

$$P = P_1 \wedge P_2$$

utilizing the properties of the inequalities of real numbers (e.g. multiplying a negative number at both sides change the direction of inequality while multiplying a positive number do not change the direction) we can write the following **true** statements.

$$P \Rightarrow Q_1$$
$$P \Rightarrow Q_2$$

in which Q_1, Q_2 are:

$$Q_1 : ac > bc$$
$$Q_2 : bc > bd$$

Since (trivially!) $bc = bc$ so we can express the following **true** statement:

$$Q_1 \wedge Q_2 \Rightarrow R$$

in which R is:

$$R : ac > bd$$

Note that we have not yet shown that $P = P_1 \wedge P_2$ implies Q (although it might trivially make sense). To arrive at the $P \Rightarrow Q$ from the baby steps, implicitly we are using the following tautology:

$$((P \Rightarrow Q_1) \wedge (P \Rightarrow Q_2) \wedge (Q_1 \wedge Q_2 \Rightarrow R)) \Rightarrow (P \Rightarrow R)$$

This is a tautology because its truth value is always true:

P	Q	R	S	$P \Rightarrow R$	$P \Rightarrow Q$	$R \wedge Q \Rightarrow S$	LHS	RHS	LHS $\Rightarrow$ RHS
0	0	0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1	1	1
0	0	1	0	1	1	1	1	1	1
0	0	1	1	1	1	1	1	1	1
0	1	0	0	1	1	1	1	1	1
0	1	0	1	1	1	1	1	1	1
0	1	1	0	1	1	0	0	1	1
0	1	1	1	1	1	1	1	1	1
1	0	0	0	0	0	1	0	0	1
1	0	0	1	0	0	1	0	1	1
1	0	1	0	1	0	1	0	0	1
1	0	1	1	1	0	1	0	1	1
1	1	0	0	0	1	1	0	0	1
1	1	0	1	0	1	1	0	1	1
1	1	1	0	1	1	0	0	0	1
1	1	1	1	1	1	1	1	1	1

Since I am in my very early phase of writing proofs for mathematical statements, I am going to do some proofs here (the questions are from the PLP book) to practice mathematical writing and thinking.

Example: Even or Odd!

Question. prove the following statements.

1. The product of two odd numbers is odd

Proof 1.
Let a, b be two odd integers. So by the definition of odd numbers we can write them as: $a = 2k + 1, b = 2l + 1$ for some integers k, l. By adding two integers and some simplification we will have: $a + b = 2(k + l + 1)$. Since $k + l + 1$ is an integer, it follows from the definition even numbers that $a + b$ is even. □

Logic Flow of the Proof 1. To make life easier, let's rewrite the statement that we want to prove:

$$T : s \text{ is the product of two odd numbers } a, b$$
$$U : s \text{ is even.}$$

so in this prove we want to evaluate the truth value of the following statement:

$$T \Rightarrow U$$

You might have guessed that the statement T does not seem to be an atomic statement (it is composite of smaller statement). So we can not directly start with the statement T and we first need to construct it with atomic sentences. Let P_1, P_2 be the following statements:

$$P_1 : \text{Integer } a \text{ is odd}$$
$$P_2 : \text{Integer } b \text{ is odd}$$

Considering the definition of the odd numbers we know that the following statements are **true**

$$I_1 : P_1 \Rightarrow Q_1 \text{ (is true)}$$
$$I_2 : P_2 \Rightarrow Q_2 \text{ (is true)}$$

in which Q_1, Q_2 are:

$$Q_1 : a = 2k + 1, \quad k \in \mathbb{Z}$$
$$Q_2 : b = 2l + 1, \quad l \in \mathbb{Z}$$

Now at this point we utilize the following **tautology**:

$$((P_1 \Rightarrow Q_1) \wedge (P_2 \Rightarrow Q_2)) \Rightarrow ((P_1 \wedge P_2) \Rightarrow (Q_1 \wedge Q_2))$$

Since I_1, I_2 are true, using the tautology above along with Modus Ponens, we can infer that the following statement is also true:

$$P_1 \wedge P_2 \Rightarrow Q_1 \wedge Q_2 \text{ (is true)}$$

Now we can construct the statement T with following **true** statement (that follows from the properties of the integer arithmetic)

$$Q_1 \wedge Q_2 \Rightarrow T$$

with T defined as before. Following the rules of arithmetic of integers numbers we can write the following **true** statement.

$$T \Rightarrow T_1 \text{ (is true)}$$

in which

$$T_1 : s = a + b = 2k + 1 + 2l + 1$$

and once again utilizing the properties of integer arithmetic, we can write the following **true** statement:

$$T_1 \Rightarrow T_2 \text{ (is true)}$$

in which T_2 is:

$$T_2 : s = 2k + 1 + 2l + 1 = 2(k + l + 1)$$

since $k + l + 1 \in \mathbb{Z}$ we can finally follow the definition of odd number, and write the following **true** statement:

$$T_2 \Rightarrow U$$

in which the statement U is as defined before. Now it is time to chain the baby statement with AND and infer the original statement. However this should be done in two steps. The first steps is to use the following tautology to infer $P_1 \wedge P_2 \Rightarrow T$ is a **true** statement:

$$(P_1 \wedge P_2 \Rightarrow Q_1 \wedge Q_2) \wedge (Q_1 \wedge Q_2 \Rightarrow T) \Rightarrow (P_1 \wedge P_2) \Rightarrow T$$

and since we now know that $P_1 \wedge P_2 \Rightarrow T$ is a true statement, assuming $P_1 \wedge P_2$ is true, then using modus ponens we can infer that T is also a **true** statement. So we will have the following conclusion from the first step:

$$T : \text{is a true statement}$$

Now here comes the second part: considering the already derived true statement and linking them by AND we can write the following **tautology**:

$$((T \Rightarrow T_1) \wedge (T_1 \Rightarrow T_2) \wedge (T_2 \Rightarrow U)) \Rightarrow (T \Rightarrow U)$$

Since the LHS of the above tautology is true, then modus ponens says the RHS should be true as well. So in summary we got:

$$T \Rightarrow U \text{ is a true statement.}$$

and since from the step 1 we know that T is true, then again modus ponens says that U is also true. □