Glossary of Proof Terms

Gratefully adapted from the work of Dr. Anders O.F. Hendrickson

The English we use in mathematics can be confusing, particularly because some words and phrases differ in meaning from their ordinary English counterparts. Since our goal is to be as precise as possible, here is a list of common phrases and the meanings they have in proofs.

Assume. See **suppose**. This is also often paired with the phrase **without loss of generality** and **for the sake of contradiction**.

By definition. This phrase is used to explain a step in a proof that is justified by the *literal definition of one of the words.* Every time you use this phrase, you should have a specific definition in mind.

By hypothesis. This phrase is used to indicate that something in your proof is true because it is one of the hypotheses. It must be referring to one of the statements in problem.

By the inductive hypothesis. If you are doing a proof by *induction*, you first prove a statement is true for the base case ($n = 1$) and then you prove that if it is true for $n - 1$, then it is true for n. The induction hypothesis is the assumption that the statement is true for $n - 1$. If you use the phrase "by the induction hypothesis", you are referring to that assumption.

By symmetry. Sometimes you need to prove two statements that are *exactly* identical, except that two variables (say x and y) change places in the argument. If the hypotheses about x and y are the same, then once you have proven the first statement, you can forgo writing the exact same proof (swapping x for y) and say that the second statement holds "by symmetry". *However, be careful! This is not the same as cases or wlog!*

Cases. One helpful technique for proof writing is the use of cases. Cases break up all possible situations into two or more options and allow for extra suppositions. For example, consider the claim that for any integer n, $n^2 - n$ is even. We can prove this with cases.

> **Claim:** Let $n \in \mathbb{Z}$ Then $n^2 - n$ is even.
> **Proof:** First note that $n^2 - n = n(n-1)$. Consider two cases: n is even or n is odd.
> Case 1: Suppose n is even. Then $2|n$, and $2|n(n-1)$.
> Case 2: Suppose n is odd. Then $n-1$ is even, $2|n-1$, and $2|n(n-1)$.

By breaking the proof into cases, we were allowed to make extra assumptions. However, note that the two cases cover *all* possibilities. If n is not even, it must be odd.

Clearly. This is a *very dangerous word!* It is often used by proof writers to cover up the fact that they have a gap in their logic. If what you are saying is so clear, why do you need to say clearly? If it's not so clear, adding the word clearly will not magically clear it up (if only!). Avoid this and similar words like "of course" and "obviously".

Conclusion. The conclusion is the statement which you are trying to prove, as opposed to the **hypotheses**, which are what you are using to prove it.

Contradiction. One of the most powerful tools in our proof toolbox is the proof by contradiction. We suppose the conclusion is false (while keeping the same hypotheses) and arrive at some sort of conflicting statement. For example, you may prove one of your hypotheses cannot hold, or something logically ridiculous like $1 = 0$.

To be absolutely clear in a proof by contradiction, you should start out by saying "Assume for the sake of contradiction" and follow it with the statement you are contradicting. Proceed with the proof, arrive at the logical inconsistency, and then complete the proof with a statement about how what you assumed must be false.

Do not confuse this with the ***contrapositive*** *of a statement!*

Contrapositive. Recall from formal logic that every statement "If P, then Q" has a *contrapositive* statement "If not Q, then not P" which is *logically equivalent* to the original statement. Sometimes proving the contrapositive is much easier than proving the original statement in that it may give us a clearer starting point for our proof.

If you choose to prove the contrapositive of a statement, always *write down the entire contrapositive!* This will help you ensure you know what you are proving.

Definition. In normal languages, a dictionary definition is just a guide to help you understand how real people actually use words. A mathematical definition is *completely different.* A mathematical definition gives a word a precise, exact mathematical formulation in terms of logic. Specifically, that word means no more and no less than what we say it does.

In particular, you should note that theorems, critical facts, and if and only if characterizations about a concept are *not* the same as the *definition* of that concept. As such, when you say " by definition" in a proof, you must be referring to some concept's precise mathematical definition.

Distinct. Synonym for different. If I say x and y are two distinct primes, it is implied that $x \neq y$.

Hypothesis. Every statement in mathematics is ultimately of the form "If..., then...". If certain hypotheses are true, then a conclusion follows. In a *claim*, we sometimes say "let" or "suppose" to indicate hypotheses. Differentiate the hypotheses (which you assume to be true) from the **conclusion** (which you need to prove to be true).

iff. Short for "if and only if", written symbolically as $\Leftrightarrow$. This is a double implication and relates two statements that are logically equivalent.

Let. When we say something like "Let x be in G", two things happen. First, we define a new object x which we get to use in our logical reasoning. Second, we nail down x as a fixed object. We can no longer add in special properties about x or define which element it is in G. We know *absolutely nothing* about x except for what is given about it in the "let" statement.

The power of the "let" statement is that it is *incredibly* general. Anything we prove about our x will be true of *every* element in G. This being said, be very particular about your "let" statements, assume no more than you need, but have enough to work with.

QED. An initialism for *quod erat demonstrandum* (which was to be shown), QED is the classical end of proof statement. You should put a symbol at the end of your proofs to inform the reader that you are done. Other options include open or filled squares, multiple lines, or tiny pictures of cats (not actually, but feel free to make up your own! I did palm trees for a while.)

Suppose. The word suppose has two subtly different uses. In a theorem statement, claim, or beginning of your proof, it sets up hypotheses. In the middle of your proof, it may set up a sub proof, contradiction, or cases.

We. In mathematics, it is traditional to use the word *we* instead of *I* in your proofs. The idea here is that you and the reader are looking at the subject together.

Without loss of generality (WLOG). Sometimes you are working through a proof with several variables, all playing identical roles in the proof so far, but you know at least *one* of them is special in some way. Consider the following example:

> **Claim:** Suppose a, b, c are positive integers and abc is even. Then $a + b + c \geq 4$.
> **Scratch Work:** Since I know abc is even, I know at least one of the variables is even. But is it a, b, or c? If I knew which one, I could probably do something more than that... Maybe I should break it into cases?

Suppose we do that. We need to refer to this special even variable by name, so we need three cases, one for each variable.

> **Claim:** Suppose a, b, c are positive integers and abc is even. Then $a + b + c \geq 4$.
> **Proof:** Since abc is even, at least one one of a, b, or c is even.
> Case 1: Suppose a is even. Then $a \geq 2$, so $a + b + c \geq 2 + 1 + 1 = 4$.
> Case 2: Suppose b is even. Then $b \geq 2$, so $a + b + c \geq 1 + 2 + 1 = 4$.
> Case 3: Suppose c is even. Then $c \geq 2$, so $a + b + c \geq 1 + 1 + 2 = 4$. $\square$

But man, this sure seems wasteful. Each case is the same, except for swapping around the letters. Enter the phrase "without loss of generality" (or wlog)! A better option is to *assume* that one of the variables is special. If it isn't, you could rewrite the proof with a different letter. For this reason, you haven't "lost generality". The proof would instead be written as:

> **Claim:** Suppose a, b, c are positive integers and abc is even. Then $a + b + c \geq 4$.
> **Proof:** Since abc is even, at least one one of a, b, or c is even. Without loss of generality, assume a is even. Then $a \geq 2$, and $a + b + c \geq 2 + 1 + 1 = 4$. $\square$

This sure does seem simpler! However, be very careful. Once you make this assumption about a, it is indeed special from that point on in the proof. You cannot say wlog about the same list of symbols more than once. Further, you must ensure that you *actually* have generality. Many a misguided student has used wlog as a means to make extra assumptions to make the proof easier. That is not how this works! With great power comes great responsibility.

($\Leftarrow$) and ($\Rightarrow$). These symbols are sometimes used to separate the two parts of an if and only if proof. They show the direction of the iff you are trying to prove at any one time.