18.700, WRITING PROOFS

One difficulty for many students of 18.700 is writing proofs. This is different from writing in other classes and different from computations on calculus problem sets. It is a skill learned through practice and feedback from graders. On the first problem sets the grader will give feedback without docking many points, but after that points will be docked appropriately. This is not a class on mathematical writing: if you have poor style but a mathematically correct proof you will receive full credit (although the graders will note the poor style). But if your logic is faulty or, more pertinently, if your write-up does not clearly communicate correct logic, you will be docked points. Following are a few writing tips as well as pitfalls to avoid.

1. Use words. Use words in your proof; do not write in computer code or a "proof table". You are writing to be read by another person, not a machine. In the same vein use complete, grammatically-correct sentences. In a longer proof use paragraphs to separate important parts of the proof. You need not write out formulas, unless this makes them more clear. But try to write out the phrases "for every", "there exists", "this implies", "is equivalent to", etc. instead of using symbolic logic notation. This will encourage you to use sentences.

2. Explain all steps. Explain all steps in your argument. A common mistake is to skip a step because you have "internalized" it and it no longer occurs to you it needs written justification. But another common mistake is to skip a step as an error of logic rather than psychology. The grader cannot tell the difference. The grader knows the correct argument, is trained in spotting gaps, and will dock points if there is a gap, no matter the reason for your mistake.

Try not to go overboard. If a step is truly obvious and is not explicitly being asked about, it can usually be omitted. If you do lose points for such an omission, you can always ask for a regrade. But you will only recover points if it is *truly obvious*; there is no use arguing with me or the grader that a nontrivial step was "obvious to you". For this reason, when you are in doubt, explain the step.

Example: Here is an example from a previous 18.700 class. Students were asked to prove for every $m \times n$ matrix A and every sequence of n-vectors $v_1, \dots, v_r$, if $Av_1, \dots, Av_r$ are linearly independent, then $v_1, \dots, v_r$ are linearly independent (all these terms will be explained in lecture soon). One write up was similar to the following.

$$\begin{aligned} (Av_1, \dots, Av_r) \ \textit{linearly independent}, \\ c_1 v_1 + \dots c_r v_r = 0, \\ c_1(Av_1) + \cdots + c_r(Av_r) = 0, \\ c_1 = \cdots = c_r = 0. \end{aligned}$$

If you were explaining the argument to a friend at a blackboard, this might be sufficient. But a clear and complete written argument looks very different.

Proof. Let $(Av_1), \dots, (Av_r)$ be a linearly independent collection of vectors in $\mathbb{F}^m$. The claim is $v_1, \dots, v_r$ is a linearly independent collection of vectors in $\mathbb{F}^n$.

Let there be given a linear relation among $v_1, \dots, v_r$,

$$c_1 v_1 + \cdots + c_r v_r = 0.$$

Date: Fall 2004.

Multiplying both sides by A,

$$A\,(c_1v_1 + \cdots + c_rv_r) = A0.$$

Clearly $A0$ equals 0. Because matrix multiplication distributes with addition,

$$A\,(c_1v_1 + \cdots + c_rv_r) = A(c_1v_1) + \ldots A(c_rv_r).$$

Because matrix multiplication commutes with scalar mutliplication this equals,

$$c_1(Av_1) + \cdots + c_r(Av_r).$$

This gives a linear relation among $(Av_1), \ldots, (Av_r)$,

$$c_1(Av_1) + \cdots + c_r(Av_r) = 0.$$

By hypothesis, $(Av_1), \ldots, (Av_r)$ is a linearly independent collection, so this is the trivial linear relation, i.e., $c_1 = \cdots = c_r = 0$. Therefore the only linear relation among $v_1, \ldots, v_r$ is the trivial linear relation, i.e., $v_1, \ldots, v_r$ is a linearly independent collection of vectors. □

Although there are formulas, they are used only if writing them out is no clearer. The assertion being proved is stated at the beginning of the argument. The reader's attention is drawn whenever a hypothesis is used. Connecting words such as "since", "so", and "therefore" are used; these keywords alert your reader you have made a deductive step. Also notice not all statements are justified, e.g. the sentence, "It is clear that $A0$ equals 0." This step is obvious enough that it needs no justification. But whenever there is doubt whether a step is obvious, explain the step.

3. State all hypotheses. Give all hypotheses in the statement of your result. On problem sets this will usually be done for you. But if a long argument includes a lemma, state all hypotheses of the lemma. You will usually need to use all hypotheses in the proof (occasionally there might be a superfluous hypothesis, but not often). When you use a hypothesis, always call attention to this fact.

4. Use correct logic. Learn and stick to the basics of logic. The "basics of logic" are such things as "If proposition 1 holds, and if proposition 1 implies proposition 2, then proposition 2 holds as well." Such basics may seem self-evident, but in a long argument they occur so often that you are bound to make a mistake unless you are diligent. On a previous 18.700 course, many students made the same logical mistake on a homework problem. They were asked to prove a set of vectors produced by a certain algorithm gives a spanning set for the intersection $W_1 \cap W_2$ of 2 linear subspaces for which spanning sets are known. Many students proved every vector in the span of the set is in $W_1 \cap W_2$. Some students proved that every vector in $W_1 \cap W_2$ is in the span of the set. But a correct argument proves every vector in the span of the set is in $W_1 \cap W_2$, and every vector in $W_1 \cap W_2$ is in the span of the set. Both implications are necessary; one alone does not suffice.

5. Use and cite definitions correctly. There are many definitions in 18.700, so it is easy to be confused. Look up definitions, use the correct names, and cite the number of the definition in the text if you are checking a long list of axioms for the definition (a common homework problem is to prove some object satisfies a definition – this is an appropriate time to cite a definition number). One common confusion in 18.700 regards the definition of *linear combination* and the definition of *span*. The sentence "the vector subspace W of the vector space V is the linear combination of the vectors $v_1, \ldots, v_n$ of V" makes no sense. The correct statement is either "the vector subspace W is spanned by the vectors $v_1, \ldots, v_n$ of V", or perhaps "every vector w in W is a linear combination of the vectors $v_1, \ldots, v_n$" (although this second statement allows the possibility that W is properly contained in the span of $v_1, \ldots, v_n$). This might seem semantical, and it is! But it is important nonetheless, and you will be docked points if you use definitions incorrectly.

6. Think the argument through before writing. Do not write in "stream-of-consciousness": you should not write all thoughts going through your mind as you solve a problem. After developing an argument for yourself, spend time rearranging the steps in correct logical order. The best order for presenting ideas is usually not the order which occurs to you first, even if that order is logical order. For example, imagine you are asked for a counterexample to the following statement, "Every integer is a difference of two square integers." One likely approach is to simply consider whole numbers in turn, $0, 1, 2$ etc., and check if these are difference of squares, e.g. $0 = 0^2 - 0^2, 1 = 1^2 - 0^2$. For 2 there is a problem. Adding some small squares to 2 does not give another square integer. Eventually it occurs to us to rewrite the equation,

$$2 = a^2 - b^2,$$

by factoring $a^2 - b^2$, i.e.,

$$2 = (a - b)(a + b).$$

Since 2 is a prime number the only possibilities are $(a - b = 1, a + b = 2)$, $(a - b = -1, a + b = -2)$, $(a - b = 2, a + b = 1)$, or $(a - b = -2, a + b = -1)$. The solution of none of these 2×2 inhomogeneous systems of equations is a vector with integer entries. Thus 2 is a counterexample.

This is *not* how to write the argument for others to read. First of all, the order is backwards: correct order states a result then gives a proof, it does not give a sequence of steps leading to a result only at the end. Also, there are several small simplifications that will save the reader time – the burden is on the author of an argument to check details and simplify arguments. One possiblity is the following.

Proof. The integer 2 cannot be expressed as a difference of two square integers. This will be proved by contradiction. By way of contradiction, suppose there exist integers a and b such that $2 = a^2 - b^2$. Factor the right-hand side of this equation as $2 = (a - b)(a + b)$. Since 2 is a prime number, either 2 divides $a - b$ or 2 divides $a + b$.

The first possibility is that 2 divides $a - b$. Either $a - b = 2$ or $a - b = -2$. Since $(-a)^2 - (-b)^2 = a^2 - b^2$, if there exists a solution with $a - b = -2$, there also exists a solution with $a - b = 2$. Thus, without loss of generality, assume $a - b = 2$. Then $a + b$ equals 1. Rewrite the first equation as $a = b + 2$ and substitute into the second equation to get $(b + 2) + b = 1$, i.e., $2(b + 1) = 1$. Because 2 does not divide 1, this is a contradiction. Thus 2 does not divide $a - b$.

The second possibility is that 2 divides $a + b$. Then either $a + b = 2$ or $a + b = -2$. For the same reason as above, without loss of generality, assume $a + b = 2$. Then $a - b$ equals 1. Rewrite this equation as $a = b + 1$ and substitute into the first equation to get $(b + 1) + b = 2$, i.e., $2(1 - b) = 1$. Again since 2 does not divide 1, this is a contradiction. Thus 2 does not divide $a + b$. Since 2 divides neither $a - b$ nor $a + b$, there is a contradiction proving 2 is not a difference of squares. □

Notice in particular it is not "left to the reader" to check $2 = (a - b)(a + b)$ has no integer solution, even though this is straightforward. Later on you will likely leave some easy calculations to your reader, but in this class explain all steps unless they are truly obvious.

7. Use proof by contradiction and proof by induction correctly. If you are using a "proof by contradiction" or a "proof by induction", say so at the beginning of the argument. In a proof by contradiction, use the keyphrase, "By way of contradiction let us assume . . ." At the end of a proof by contradiction, after deducing an absurdity by assuming the negation of the statement to be proved, say something like, "This result is absurd. Therefore we conclude our original hypothesis is false, which is to say . . ." and then repeat the statement to be proved. The proof is complete only after you have explained how the absurdity leads to the statement you wanted. There is a further remark about proof by contradiction below.

In a proof by induction, always remember the *base case*, or the step "n equals 1" (or possibly n equals 0 or some other integer depending on the exact statement to be proved). Present the base case before the induction step. After that state the induction hypothesis and say you are doing so. Use a sentence like, "By way of induction, suppose the result is known for the integer n." Explain how the hypotheses of the theorem together with the induction hypothesis implies the result for $n + 1$. Call attention to the exact step (or steps) in the argument where the induction hypothesis is used. If it is *not* used, you should not present the argument as proof by induction even if it is logically valid to do so: you only confuse the reader by presenting a direct argument as proof by induction.

Pitfalls of proof by contradiction: Some mathematicians (admittedly a small minority) reject proof by contradiction. Even without this, as a matter of style never use proof by contradiction if there is a comparably simple direct proof. Some use proof by contradiction as a labor-saving device: They state all hypotheses, assume the negation of the theorem, write down alot of steps (sometimes incoherent, often difficult to follow), eventually deduce an absurdity, and then claim to have given a valid argument. This is unacceptable: the responsibility for doing the work of the argument and presenting a clear proof is on the author, not the reader. There is another, more serious pitfall: proof by contradiction is not *robust.* Any logical mistake by the author, no matter how minor, is likely to lead to a contradiction somewhere in the argument. In a direct proof the author sees the contradiction, back-tracks to the mistake, and corrects it. In proof by contradiction, the author mistakenly assumes the contradiction gives a valid proof. For this reason *every* mathematician is wary of proof by contradiction, not just those who reject it outright. Sometimes proof by contradiction is unavoidable; use it only in these cases.

These are a few of the rules you should learn and use in writing proofs. There are many others. The best way to learn them is to read proofs: both good and bad. Good proofs are easy to find; just pick up most textbooks or math journals (you do not need to understand the mathematics involved to appreciate the style of a well-written argument). Bad proofs, unfortunately, are also easy to find. It is a matter of patience, practice and experience to produce good arguments and not bad ones.