The Nesbitt-Johnston Writing Center
Hamilton College
Clinton, NY 13323

Acknowledgements: This handout is primarily the work of Phillip J. Milner'10, with generous assistance from the Mathematics Department (especially Prof. Sally Cockburn), Sharon Williams, and Dave Foster'10.

Mathematical Proofs: Where to Begin And How to Write Them

Starting with Linear Algebra, mathematics courses at Hamilton often require students to prove mathematical results using formalized logic. This can occasionally be a difficult process, because the same statement can be proven using many different approaches, and each student's proof will be written slightly differently. What is the correct way to write a mathematical proof? The answer is a matter of taste (taste you will acquire with practice...lots of practice), but there are universal do's and don't's and good places to get started with your proofs. This handout seeks to clarify the proof-writing process by providing you with some tips for where to begin, how to format your proofs to please your professors, and how to write the most concise, grammatically correct proofs possible.

The Proof-Writing Process

1. A proof must **always** begin with an initial statement of what it is you intend to prove. It should **not** be phrased as a textbook question ("Prove that…."); rather, the initial statement should be phrased as a theorem or proposition. It should be self-contained, in that it defines all variables that appear in it. After you've written what it is you're proving, you should begin the proof itself with the notation *Proof:* or *Pf:*. End with notation like *QED*, *qed*, or *#*.

Example: The question tells you to "Prove that if x is a non-zero element of **R**, then x has a multiplicative inverse." Your proof should be formatted something like this:

If x is a non-zero element of **R**, then x has a multiplicative inverse.
Pf: [Insert proof here]. QED

Luckily, the initial statement is the best place to begin your thought process, because it forces you to ask the question "What am I trying to prove?" Elements of a given set have a particular property? To provide a counterexample disproving that a given set has a given property? The best place to start is to **understand what it is you are proving** and, more importantly, **what mathematical entity you have to work with**.

2. **Always introduce your variables**. The first time a variable appears, whether in the initial statement of what you are proving or in the body of the proof, you must state what kind of variable it is (for example, a scalar, an integer, a vector, a matrix), and whether it is universally or existentially quantified. For example, "there exists some $k \in \mathbf{Z}$ such that …" or "for any $a \in A$." Note that if you write "let $a \in A$," you are implying that what follows is true for **any** $a \in A$.

Most mathematical propositions are **universally quantified implications** of the form "For all [objects of a particular type], if [hypothesis], then [conclusion]." (Symbolically, this is "$\forall x \in D,\ p(x) \Rightarrow q(x)$"). Even if it is not obvious that what you are proving is a statement of this form, (i.e. it doesn't contain the exact words "For all...if...then..."), it **probably** still is. For example, the statement "All bounded sequences have a convergent subsequence" is really the statement "For all sequences $(x)_n$, if $(x)_n$ is bounded then $(x)_n$ has a convergent subsequence." Thus, a good place to start your proof is to **restate what you are proving as a universally quantified**

implication. An implication is true for all $x \in D$ if it is true for a 'Joe Average' $x \in D$, so you should begin the proof of such a statement with "Let $x \in D$." Thus, for our proof of the statement above, we would start with "Let $(x)_n$ be a sequence." *Do not assume anything about x except that it belongs to D!* In particular, **do not let x be a specific number or matrix or vector.** For example, we don't assume that $(x)_n$ is a specific sequence, because we want the proof to be true for **all** sequences, not just that specific one. This also holds for "if and only if" statements.

3. Now that you have your universally quantified implication, there are three common strategies for proving the implication is true and only one for proving it is false; these are outlined here. Note that direct proofs are preferred whenever possible, and that direct proofs and proofs by contrapositive are far more common than proofs by contradiction.

i. In a direct proof, the first thing you do is explicitly assume that the hypothesis is true for your selected variable, then use this assumption with definitions and previously proven results to show that the conclusion must be true.
Direct Proof Walkthrough: Prove that if a is even, so is a^2. *Universally quantified implication: For all integers a, if a is even, then a^2 is even.*
Claim: If a is even, so is a^2.
Pf: Let a be an integer, and assume it is even. *Now ask: what does this mean? An integer being even means that it is divisible by 2, or, equivalently, that there exists an integer k such that a = 2k.* By definition, there exists an integer k such that a = 2k. *Now look at what we are proving – that a^2 is even. We do this by proving that a^2 is divisible by 2.* Hence, $a^2 = (2k)^2 = 4k^2$. Since 4 is divisible by 2, this implies that a^2 is also divisible by 2, and so it is even by definition. QED *This proof illustrates the basic principle behind a direct proof – start with what you know, and ask "what do I have to show to reach the conclusion?" In this case, we needed to show that a^2 was divisible by 2, knowing that a was.*

ii. In a **proof by contrapositive**, you **explicitly** assume that the conclusion is false for your variable, then use this assumption, plus definitions and proven results, to show that the hypothesis must be false for your chosen variable. Remember that **the contrapositive of an implication is logically equivalent to the original implication**, so this is an indirect method for showing that the original implication is true. Use when the negative of a definition in your implication is easier to work with than what is given. A good example is linear dependence, which only means that a set is not linearly independent. If you use the contrapositive, you are working with linear independence, which is a set definition with many theorems tied to it, making it much easier to work with.
Proof by Contrapositive Walkthrough: Prove that if a^2 is even, then a is even.
Claim: If a^2 is even, then a is even.
Pf: *The problem here is that the fact that a^2 is divisible by 2 does NOT directly lead us to the fact that a is even, since $a^2 = 2k$ only gives us that $a = \sqrt{2k}$, which does not imply that a is even. Because we would rather work with a, we should try a proof by contrapositive. Start by assuming the negation of the conclusion, which states that a is even.* Let a be an integer, and assume a is odd. *Now we want to show that a^2 is odd. This is now just a direct proof of the implication "If a is odd, then a^2 is odd," and we follow the same strategy as that above.* By definition, there exists an integer k such that a = 2k + 1. Hence, $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. Note that whether k^2 is even or odd, $4k^2$ and 4k are both divisible by 2, and so $4k^2 + 4k$ is divisible by 2 as well. Hence, $4k^2 + 4k$ is even by definition. This implies that $a^2 = 4k^2 + 4k + 1$ is odd. QED

iii. In a **proof by contradiction**, the first thing you do is **explicitly assume that the implication is false**; that is, you assume that the hypothesis is true but the conclusion is false for your selected variable. Then use *both* of these assumptions to arrive at a contradiction of some *other* proven result. Because you know the other proven result **must** be true, you must conclude that your original assumption that the conclusion was false was incorrect; in other

words, you are indirectly proving that the original implication is true by showing that it cannot possibly be false. Proofs by contradiction are useful for showing that something is impossible and for proving the converse of already proven results. Proofs by contradiction can be somewhat more complicated than direct proofs, because **the contradiction you will use to prove the result is not always apparent from the proof statement itself.**

Proof by Contradiction Walkthrough: Prove that $\sqrt{2}$ is irrational.

Claim: $\sqrt{2}$ is irrational.

Pf: *Here we are proving something about a specific number, so we do not start with a "let" statement or a universally quantified implication. Since were trying a proof by contradiction, we start by assuming the* ***opposite*** *result of the one we are trying to show*. Assume that $\sqrt{2}$ is rational. *What does this mean?* By definition, there exist integers p and q such that $\sqrt{2} = p/q$. Since every fraction can be reduced to smallest terms, assume that p and q have no common divisors so that p/q is the simplest fraction $\sqrt{2}$ equals. *This is the outside assumption* ***that is not part of the hypothesis*** *we are going to contradict.* This implies that

$(\sqrt{2})^2 = (p/q)^2$, which implies that

$2 = p^2/q^2$, which implies that

$2q^2 = p^2$.

By definition, p^2 is even, which implies that p is even by our Contrapositive Proof above. Hence, there exists an integer k such that $p = 2k$. Substituting this in, we get:

$$(\sqrt{2})^2 = (p/q)^2 \rightarrow$$
$$2 = (2k/q)^2 \rightarrow$$
$$2 = 4k^2/q^2 \rightarrow$$
$$2q^2 = 4k^2 \rightarrow$$
$$q^2 = 2k^{2.}$$

By definition, then, q is even. However, this is a contradiction of the fact that p/q is a fraction in lowest terms, since p and q are both divisible by 2 by definition. *Make sure you always explicitly state what it is you are contradicting! Technically, you do not need to conclude with "Hence, $\sqrt{2}$ irrational," but some professors may like you to do so anyways.* QED

REMEMBER: If you use ONLY the assumption that the hypothesis is true to end up with the "contradiction" that the hypothesis is false when you assumed it to be true, then what you have is a proof by contrapositive, not a proof by contradiction!

To prove a statement of the form "$\forall x \in A,\ p(x) \Rightarrow [q(x) \vee r(x)]$," the first thing you do is explicitly assume $p(x)$ is true and $q(x)$ is false; then use these assumptions, plus definitions and proven results to show that $r(x)$ must be true. For example, to prove the statement "If x is an integer, then $x \in \mathbf{N}$ or $x \leq 4$," you would assume that x is an integer and that x is not a natural number, and then try to prove that x must be less than or equal to 4 (you can argue the opposite as well).

To **disprove** a universally quantified statement, it suffices to find **one, specific** counterexample. The simpler the counterexample, the better! **Do not try to find a general argument for why the statement is false.**

Grammatical Rules for Writing Proofs

1. **ALWAYS** write in complete, grammatically correct sentences, just as you would in any other subject (this means that all the grammar rules you learned in English class still apply here). **A sentence must begin with a WORD, not with mathematical notation** (such as a numeral, a variable or a logical symbol). This cannot be stressed enough – every sentence in a proof must begin with a word, not a symbol! **A sentence must end with PUNCTUATION**, even if the sentence ends with a string of mathematical notation. Even chunks of mathematical notation must be grammatically correct, which means that mathematical symbols must fit into the logical flow of your sentences. To test this, try reading your statements involving mathematical symbols out loud.

Example: "Since x is a vector → x has a magnitude." Read this sentence out loud, replacing the implication symbol with what it stands for – does it make sense? This sentence construction is a common error; the hypothesis and conclusion of an implication **must be independent statements**. In this case, the word since is redundant.

2. Do not 'wrap' mathematical expressions on two or more lines inside your prose; instead, separate long mathematical expressions from the text on indented lines (as you would with long quotations in an essay), with equals signs /inequality signs lined up vertically.

Example: "….Note that $2x = x^2 - 4x \rightarrow 2 = x - 4 \rightarrow x = 6$."

This is incorrect! Do not wrap mathematical statements around two lines. Instead, do this:

"…Note that $2x = x^2 - 4x \rightarrow$
$2 = x - 4 \rightarrow$
$6 = x$."

3. Some professors do not allow you to use the symbols $\exists$ and $\forall$ in formal writing (unless the question specifically asks for symbolic logic notation). Make sure to ask your professor if there is any doubt!

4. Don't 'pad' your answers; good mathematical writing is both thorough and **concise**. Ideally, your proof should contain only necessary statements and the logical steps between them. This includes wishy-washy conceptual statements that are irrelevant to the logical structure of your proof (see Example). Take advantage of mathematical notation to cut down on excess words; for example, instead of writing "let *x* be an element of the set of natural numbers", simply write "let $x \in \mathbf{N}$". Just like in other classes, you should avoid empty phrases such as "it can be seen that..." or "we are able to show that..." and statements in which you "rephrase" mathematical symbols into standard English; they usually add nothing to your argument. Finally, **do not use a concluding sentence reiterating what you set out to prove**; the logical structure of your proof should make it amply clear when you are done. In essence, treat your proofs like you would a short essay in an English or Philosophy class – include only what is necessary to demonstrate the logical progression of your proof, and as little else as possible.

Example: Let V and W be vector spaces, and suppose $T : V \rightarrow W$ is a one-to-one linear transformation. Prove: if $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a linearly independent subset of V, then the set $\{T(\mathbf{u}), T(\mathbf{v}), T(\mathbf{w})\}$ is a linearly independent subset of W.

Wrong Proof: If a function is one-to-one, then we know that for nonzero vectors **a** and **b**, if $\mathbf{a} \neq \mathbf{b}$ then $T(\mathbf{a}) \neq T(\mathbf{b})$, by definition. Since $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is a linearly independent subset of V, no vectors in this subset can be expressed as a linear combination of another vector in the subset, and thus each vector is distinct. Then, we know that since $\mathbf{u} \neq \mathbf{v} \neq \mathbf{w} \neq \mathbf{u}$, $T(\mathbf{u})$, $T(\mathbf{v})$, $T(\mathbf{w})$ are distinct vectors. But is the set $\{T(\mathbf{u}), T(\mathbf{v}), T(\mathbf{w})\}$ linearly independent? Suppose that it is linearly dependent…[continues on correctly].

What's wrong: The author does not begin by stating his variables (where do **a** and **b** come from?), and seems to ramble a bit in thought. In fact, this proof contains the sort of *conceptual* work that, while important for writing the proof, **is not necessary** to show in the proof (*i.e.* its several statements of what linearly independent means). Indeed, not until several sentences into the proof do we get an idea of where it is going: "Suppose that [the set] is linearly dependent…" suggests that this is either a proof by contrapositive or contradiction, most likely the latter. However, the assumption of the hypothesis is **never clearly made.** Lastly, this proof is very wordy; the entire proof can be written in a shorter space than this introductory section!

Right Proof (by contrapositive): Suppose $\{T(\mathbf{u}), T(\mathbf{v}), T(\mathbf{w})\}$ is linearly dependent. Then there exist scalars a and b such that $T(\mathbf{u}) = aT(\mathbf{v}) + bT(\mathbf{w})$ by definition. By the properties of linear transformations, $T(\mathbf{u}) = aT(\mathbf{v}) + bT(\mathbf{w}) = T(a\mathbf{v}) + T(b\mathbf{w}) = T(a\mathbf{v} + b\mathbf{w})$. Since T is one-to-one, $\mathbf{u} = a\mathbf{v} + b\mathbf{w}$ by definition. This implies that $\{\mathbf{u},\mathbf{v},\mathbf{w}\}$ is linearly dependent by definition. QED

This proof is short, succinct, and logical, containing no unnecessary details. However, it still has complete, grammatically correct sentences and flows nicely. This is the ideal to which you should strive!