Math 19
Winter 2020
Some Proof Principles

Generally, proving something requires some creativity; there is no recipe for producing a proof. However, there are some standard techniques that can be used, depending on the form of the statement you are trying to prove. (Note that "can" does not mean "must.") Here are a few of them.

1. To prove a statement of the form "If P, then Q," assume P and prove Q. Or, prove the *contrapositive*, "If not Q, then not P," by assuming not Q and proving not P.

2. To prove a statement of the form "P if and only if Q" ($P \iff Q$), prove "If P, then Q," and prove, "If Q, then P."

3. To prove a statement of the form "not P," use *proof by contradiction*: Assume P, and deduce a contradiction, something obviously false or contradictory.

4. To prove a statement of the form "For all sets x, P(x)," let x be a name for an arbitrary set, and prove P(x). Be careful not to make any special assumptions about x.

5. To prove a statement of the form "There is a set x such that P(x)," find a specific example B and prove that P(B). (For example, prove that P($\emptyset$).)

6. To prove a statement of the form "P and Q," prove both P and Q.

7. To prove a statement of the form "P or Q," prove "If not P, then Q," or prove "If not Q, then P," or assume "Not P and not Q" and deduce a contradiction. Or, consider all possible cases, and prove that in some cases P holds, and in other cases Q holds.

8. In general, prove something by considering all possible cases separately. You must be sure the cases you list cover all possibilities. There is an example of a proof using this on page 5 of this handout.

9. To prove something is unique, assume there are two such things, and prove they are actually equal.

10. To prove a statement of the form "There is a unique x such that P(x)," prove both "There is an x such that P(x)" and "the x such that P(x) is unique." This is called proving existence and uniqueness.

11. To prove two sets A and B are equal, prove that every element of A is also an element of B, and every element of B is also an element of A. (This is unlike the preceding items, because it uses not only logic – reasoning from the definitions of the logical notions "for all," "there exists," "implies," and so forth, considering = to be a logical notion – but also the principle of extensionality for sets.)

Example: Prove that for every real number a there is a unique degree 2 polynomial $f(x)$ such that $f(0) = f'(0) = f''(0) = a$.

Proof: Let a be an arbitrary real number.[1] We must prove the existence and uniqueness of a degree 2 polynomial $f(x)$ with the given property.

First we prove existence. Let $f(x) = \frac{a}{2}x^2 + ax + a$. This is a degree 2 polynomial. Computing the first two derivatives gives $f'(x) = ax + a$ and $f''(x) = a$. Substituting 0 for x gives $f(0) = a$, $f'(0) = a$, and $f''(0) = a$. This is what we needed.[2]

To prove uniqueness, suppose that the degree 2 polynomial $g(x) = bx^2 + cx + d$ also has $g(0) = g'(0) = g''(0) = a$. We must show that g equals f.[3]

Computing the derivatives of g gives $g'(x) = 2bx + c$ and $g''(x) = 2b$. Substituting 0 for x, and using $g(0) = g'(0) = g''(0) = a$, gives $g(0) = d = a$, $g'(0) = c = a$, and $g''(0) = 2b = a$, so $b = \frac{a}{2}$. This gives $g(x) = bx^2 + cx + d = \frac{a}{2}x^2 + ax + a$. Therefore, g equals f, which is what we needed to show.

[1] We are using (4) from the previous page. We are about to use (10) as well, proving existence and uniqueness.

[2] We are using (5) from the previous page, showing a particular degree 2 polynomial has the given property.

[3] We are using something like (9) from the previous page, showing any other degree 2 polynomial with the given property must equal the one we already found.

Writing Proofs

A mathematical proof of a statement is a clear, complete, and logically correct argument that the statement must be true. Here are a few important points about proofs:

1. Proofs are written in mathematical English. This means you should use complete sentences with correct grammar and punctuation.

2. You should use mathematical formulas, equations, and pictures in a proof, whenever they help make your proof readable and understandable.

3. Formulas, equations, and pictures should always be explained. A string of equations without explanations is not a proof.

4. Formulas and equations are included in sentences, and must be punctuated accordingly. Notice the punctuation in the following proof.

5. Always begin by stating the proposition you are going to prove.

6. Make the logic of your proof clear to your reader. If you are proving that P implies Q, it is good to begin with, "Assume P. We will prove Q."

7. How your proof is laid out on the paper matters. Centering long mathematical expressoins on their own lines, and skipping lines between parts of a solution, can make your solution much more readable. Neatness counts.

8. It is fine to use formulas and results from the text or from class. Be sure you reader knows what axiom, formula, or result you are using.

9. There is generally more than one correct proof of a theorem, and more than one way to write up a given proof. Unless a homework or exam problem specifies a particular approach or technique, you can use any logically valid method of proof

10. The amount of detail needed in a proof depends on the intended reader. For this class, your intended reader should be a student in the class who does not understand the material quite as well as you do.

11. The mathematical "we" is common in proofs, but it is fine to use "I," as in, "Let $\vec{a}$ be an additive identity. I will prove that $\vec{a} = \vec{0}$

12. The meaning of any symbols you use should always be clear. ("Clear" does not mean "you can figure it out from context." It means *clear*.)

13. Professor Annalisa Crannell of Franklin and Marshall College has written a booklet about writing mathematics for her calculus classes. She discusses a number of strategies and conventions for writing mathematics well. You can find her booklet at

    https://www.fandm.edu/uploads/files/107682389602454187-guide-to-writing.pdf.

    Professor Steven Kleiman of MIT has written a more advanced guide to writing mathematics, intended for undergraduate students who are writing mathematical papers. You can find his guide at

    http://www.mit.edu/afs/athena.mit.edu/course/other/mathp2/www/piil.html.

14. Excellent mathematical writing style embodies several characteristics, of which the three most important are clarity, clarity, and clarity. It is important to use words precisely and correctly. Generally, simple declarative sentences and consistent word use are preferable to variation in sentence structure and vocabulary. The same is true of most technical writing; the deeper and more complex the ideas, the simpler and more transparent the writing should be. My favorite quotation about this comes from the web page "Guidelines for Writing a Phiilosophy Paper" by NYU philosophy professor James Pryor:[4]

    > If your paper sounds as if it were written for a third-grade audience, then you've probably achieved the right sort of clarity.

[4]http://www.jimpryor.net/teaching/guidelines/writing.html

Proposition: For all sets A, B, and C,

$$(A \cap C) \cup (B \cap C) \subseteq (A \cup B) \cap C.$$

Proof: We must show that every element of $(A \cap C) \cup (B \cap C)$ is also an element of $(A \cup B) \cap C$.[5]

Suppose x is an arbitrary element of $(A \cap C) \cup (B \cap C)$. We must show $x \in (A \cup B) \cap C$. By the definition of union, since $x \in (A \cap C) \cup (B \cap C)$, either $x \in (A \cap C)$ or $x \in (B \cap C)$.

Case 1: $x \in A \cap C$. Then $x \in A$ and $x \in C$. Since $x \in A$, we also have $x \in A \cup B$. Now we have both $x \in A \cup B$ and $x \in C$, so $x \in (A \cup B) \cap C$.

Case 2: $x \in B \cap C$. By the same reasoning, $x \in A \cup B$ and $x \in C$, so $x \in (A \cup B) \cap C$.

This completes the proof.

Exercise: Provide the following proof. You can either work together to write a proof, or each write a proof, and then read each other's proofs and give feedback about how clear and easy to read they are. Note that these two propositions together prove a distributive law, intersection distributes over union:

$$(A \cap C) \cup (B \cap C) = (A \cup B) \cap C.$$

Proposition: For all sets A, B, and C,

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C).$$

Proof:

[5] This proof is assuming a certain level of understanding in the reader, by not explicitly stating, "Let A, B, and C be arbitrary sets." The level of sophistication you should assume in your reader, for this course, is that of another Math 19 student who doesn't understand things quite as well as you do.

Exercise: Show that for all sets A and B we have $\mathcal{P}(A \cap B) = (\mathcal{P}A) \cap (\mathcal{P}B)$. For this exercise, everybody try writing down a proof, and then compare notes.