Math 38
Spring 2016
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 A, then B," assume A and prove B. Or, prove the *contrapositive*: "If not B, then not A," by assuming not B and proving not A.

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

3. To prove a statement of the form "For all vectors x, A(x)," let x be a name for an arbitrary vector, and prove A(x).

4. To prove a statement of the form "There is a vector x such that A(x)," find a specific example $\vec{v}$ and prove that A($\vec{v}$). (For example, prove that A($\vec{0}$).)

5. To prove a statement of the form "A and B," prove both A and B.

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

7. 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 like this later in this document.

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

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

Proof by Mathematical Induction

Mathematical induction is used to prove a statement of the form, "For every natural number n, $P(n)$." The proof then has two steps:

Base Case: Prove $P(1)$.

Inductive Step: Assume that n is a natural number such that $P(n)$. (This is the inductive hypothesis.) Prove $P(n+1)$.

(In other words, prove that for any natural number n, if $P(n)$, then $P(n+1)$.)

This works, because once we prove both $P(1)$ and $(P(n) \implies P(n+1))$, it follows that $P(2)$. From $P(2)$ and $(P(n) \implies P(n+1))$, it follows that $P(3)$. From $P(3)$ and $(P(n) \implies P(n+1))$, it follows that...

In this way, all the natural numbers fall into line like dominoes, and we conclude that $P(n)$ holds for every natural number n.

An alternative form of mathematical induction, which will be very useful to us, is strong induction. A proof by strong induction has the following two steps:

Base Case: Prove $P(1)$.

Inductive Step: Assume that n is a natural number such that $P(j)$ for every natural number $j < n$. (This is the inductive hypothesis.) Prove $P(n)$.

(In other words, prove that for any natural number n, if $P(j)$ for every natural number $j < n$, then $P(n)$.)

The textbook discusses strong induction on page 19.

Note: In Math 38, we will often say we will prove propositions of the form "$P(G)$ holds for every finite graph G" by induction on, for example, the number of vertices in the graph. This means that we are proving, by induction on n, the proposition "$P(G)$ holds for every graph G with n vertices."

Writing 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 the additive identity of a vector space is unique, it is better to begin with, "Let $\vec{a}$ be an additive identity. We will prove that $\vec{a} = \vec{0}$," than to begin with merely, "Let $\vec{a}$ be an additive identity."

7. How your proof is laid out on the paper matters. Centering equations 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 your 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 every symbol you use should 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 here:

https://edisk.fandm.edu/annalisa.crannell/writing_in_math/guide.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 here:

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:[1]

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

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

Proposition: Suppose that $X \subseteq \mathbb{R}^2$ is a subspace of $\mathbb{R}^2$. (That is, X, with the same addition and scalar multiplication as in $\mathbb{R}^2$, is itself a vector space over $\mathbb{R}$.) Then X must be one of:

1. the zero vector space, $\{\vec{0}\}$;
2. a line through the origin;
3. all of $\mathbb{R}^2$.

Proof: There are three possible cases for X:

1. X contains no nonzero vectors;
2. X contains at least one nonzero vector, and all nonzero vectors in X are parallel;
3. X contains at least one pair of nonzero vectors that are not parallel.

We consider each case separately.

1. We will show that if X contains no nonzero vectors, then X is the zero vector space.

   X must contain at least one vector, by the vector space axiom asserting the existence of an additive identity. Therefore, since X does not contain any nonzero vectors, X must contain the zero vector, and we have $X = \{\vec{0}\}$. That is, X is the zero vector space.

2. We will show that if X contains at least one nonzero vector, and all nonzero vectors in X are parallel, then X is a line through the origin.

   Let $\vec{v}$ be some nonzero element of X. If $\vec{w}$ is any other element of X, either $\vec{w} = \vec{0}$ or $\vec{w}$ is parallel to $\vec{v}$. In either case, $\vec{w}$ is a scalar multiple of $\vec{v}$; that is, $\vec{w} = t\vec{v}$ for some scalar t. This shows that every element of X is a scalar multiple of $\vec{v}$.

   Now, because X is a vector space, X is closed under multiplication by scalars, so *every* scalar multiple of $\vec{v}$ must be in X. Therefore X must consist exactly of all the scalar multiples of $\vec{v}$,

   $$X = \{t\vec{v} \mid t \in \mathbb{R}\}.$$

   That is, X is the line through the origin in the direction of $\vec{v}$.

3. We will show that if X contains contains at least one pair of nonzero vectors that are not parallel, then X is all of $\mathbb{R}^2$.

   Let $\vec{v}$ and $\vec{w}$ be nonzero, nonparallel elements of X. Because X is closed under both addition and multiplication by scalars, every vector of the form $s\vec{v} + t\vec{w}$ must be in X. To show $X = \mathbb{R}^2$, we must show every vector $(c_1, c_2) \in \mathbb{R}^2$ can be written in the form $s\vec{v} + t\vec{w}$.

Method 1: Argue geometrically. Since $\vec{v}$ and $\vec{w}$ are not parallel, you can get from $(0, 0)$ to any point in the plane by proceeding some distance in the direction of $\vec{v}$ and then some distance in the direction of $\vec{w}$. That is, you can express any element of $\mathbb{R}^2$ as the sum of a scalar multiple of $\vec{v}$ and a scalar multiple of $\vec{w}$.

Method 2: Argue algebraically.

Suppose $\vec{v} = (a_1, a_2)$ and $\vec{w} = (b_1, b_2)$. We must show that for any choice of (c_1, c_2) we can find real numbers s and t such that

$$s(a_1, a_2) + t(b_1, b_2) = (c_1, c_2).$$

That is, we must show we can always solve the system of linear equations

$$a_1 s + b_1 t = c_1$$

$$a_2 s + b_2 t = c_2$$

for s and t.

We claim that if $a_1 b_2 = a_2 b_1$, then $\vec{v}$ and $\vec{w}$ are parallel. Check this by cases:

(a) If $a_1 = 0$, then $a_1 b_2 = 0$, so by assumption $a_2 b_1 = 0$. Since $(a_1, a_2) = \vec{v} \neq (0, 0)$, and $a_1 = 0$, we must have $a_2 \neq 0$, and so $b_1 = 0$. In this case, $\vec{v} = (0, a_2)$ and $\vec{w} = (0, b_2)$ are parallel.

(b) If $a_2 = 0$, a similar argument shows $\vec{v}$ and $\vec{w}$ are parallel.

(c) If $a_1 \neq 0$ and $a_2 \neq 0$, we can divide $a_1 b_2 = a_2 b_1$ by $a_1 a_2$ to get

$$\frac{b_2}{a_2} = \frac{b_1}{a_1} = d,$$

from which we have

$$d(a_1, a_2) = (da_1, da_2) = \left(\frac{b_1}{a_1} a_1, \frac{b_2}{a_2} a_2 \right) = (b_1, b_2),$$

showing $\vec{v}$ and $\vec{w}$ are parallel.

Since $\vec{v}$ and $\vec{w}$ are not parallel, $a_1 b_2 \neq a_2 b_1$, and so $a_1 b_2 - a_2 b_1 \neq 0$, In that case, we can check that

$$s = \frac{c_1 b_2 - c_2 b_1}{a_1 b_2 - a_2 b_1} \qquad t = \frac{a_1 c_2 - a_2 c_1}{a_2 b_2 - a_2 b_1}$$

is a solution of the system of linear equations.

This is what we needed to show to complete the argument for Case 3. Therefore, this completes the proof.

Proposition: Let a and r be real numbers, and $r \neq 0$. For every natural number n,

$$\boxed{\sum_{i=0}^{n} ar^i = a\frac{1-r^{n+1}}{1-r}.}$$

Proof: We will prove this by induction on n.

Base Case: We must prove $\boxed{\sum_{i=0}^{1} ar^i = a\frac{1-r^{1+1}}{1-r}}$. To show this, we write:

$$\sum_{i=0}^{1} ar^i = ar^0 + ar^1 = a(1+r) = a\frac{(1-r)(1+r)}{1-r} = a\frac{1-r^2}{1-r} = a\frac{1-r^{1+1}}{1-r}.$$

This is what we needed to show.

Inductive Step: Assume that n is a natural number such that $\boxed{\sum_{i=0}^{n} ar^i = a\frac{1-r^{n+1}}{1-r}}$. (This is the inductive hypothesis.) We must show $\boxed{\sum_{i=0}^{n+1} ar^i = a\frac{1-r^{n+1+1}}{1-r}}$. To show this, we write:

$$\sum_{i=0}^{n+1} ar^i = \sum_{i=0}^{n} ar^i + ar^{n+1}.$$

Now we use our inductive hypothesis to write:

$$\sum_{i=0}^{n} ar^i + ar^{n+1} = a\frac{1-r^{n+1}}{1-r} + ar^{n+1} =$$

$$a\frac{1-r^{n+1}}{1-r} + a\frac{r^{n+1}(1-r)}{1-r} = a\frac{1-r^{n+1}}{1-r} + a\frac{r^{n+1}-r^{n+1+1}}{1-r} = a\frac{1-r^{n+1+1}}{1-r}.$$

This gives us $\sum_{i=0}^{n+1} ar^i = a\frac{1-r^{n+1+1}}{1-r}$, which is what we needed to show.

This completes the proof. $\square$

Notes on proof by induction:

1. The general structure of a proof by induction is something like:

   > Proposition: [Perhaps state some initial assumptions.] For all natural numbers n, $P(n)$.
   >
   > Proof: We will prove this by induction. [Or, if there are other variables in the statement of the proposition, especially other variables that represent natural numbers, we can write "We will prove this by induction on n."]
   >
   > Base Case: We must prove $P(1)$. [...][2]
   >
   > Inductive Step: Assume that n is a natural number such that $P(n)$. (This is the inductive hypothesis.) We must show $P(n+1)$. [...]
   >
   > (Inductive Step for Strong Induction: Assume that n is a natural number such that $P(j)$ for every natural number $j < n$. (This is the inductive hypothesis.) We must show $P(n)$. [...])

   In the example proof, I used these words, substituting $\displaystyle\sum_{i=0}^{n} ar^i = a\frac{1-r^{n+1}}{1-r}$ for $P(n)$.

2. Note that the boxed equation in the statement of the proposition is my $P(n)$. (In general, $P(n)$ may contain words as well as symbols.) I use *exactly* the same statement of $P(n)$, word for word and symbol for symbol (except for replacing n by 1 in the base case, and by $n+1$ in the inductive step) later in the proof.

   I wrote $0+1$ and $n+1+1$, rather than 1 and $n+2$, to emphasize the fact that I get the statements I need to prove from the statement of $P(n)$ by simply plugging in 1 for n (in the base case) and $n+1$ for n (in the inductive step). In the real world of mathematical writing, I would write 1 and $n+2$, and expect my reader to realize that these are $0+1$ and $n+1+1$.

   If this were homework, you could write whichever makes most sense to you.

3. Notice how I incorporated a string of computations into a proof written in complete sentences. You can also say things like, "We see this from the following sequence of equations," or "We demonstrate this by the following two-column proof."

   Notice that I still use punctuation.

4. To be more explicit, if I were writing for a reader not completely comfortable with proof by induction, I could have begun by base case with, "We must prove the statement holds for $n = 1$. That is, we must prove $\displaystyle\sum_{i=0}^{1} ar^i = a\frac{1-r^{1+1}}{1-r}$." I could similarly

[2] Often the base case is $n = 0$ rather than $n = 1$. If you are proving $P(n)$ holds for all integers $n \geq b$, your base case is $n = b$.

have begun my inductive step with, “We assume the statement holds for some natural number n, and we must prove it holds for $n+1$. That is, …”

Again, you can do whichever makes more sense to you.

5. This is an example of careful, formal mathematical writing, such as might be incorporated into a paper. Usually, in homework, you can get away with being a little less careful about using complete sentences, as long as your language remains readable and clear. For example, it is pretty standard to write:

   Proof: By induction on n.

   or

   Proof: By induction on the number of vertices in G.

   However, in homework for me, you cannot get away with using $\Longrightarrow$ to mean “and from this it follows that…” The symbol $\Longrightarrow$ means “implies.” If you mean “and from this it follows that…” you can write “and therefore…”

   To elaborate: $A \implies B$ means “If A, then B.” It does not mean that either A or B is true. If you mean to say that A is true, and it follows from that that B is true, you can say “A, and therefore B.”