Some Strategies for Proving Things

The Limits of Logic (PHIL 450)

Fall 2018

One of the central skills of this course is showing that certain statements are true, by giving very careful arguments from clearly specified premises, at a very high standard of precision. The way we do this is with *informal proofs*. Here "informal" contrasts with the *formalized* proofs that we will discuss in Chapter 7, and which you may have practiced in previous logic classes. We are writing our arguments in clear English, rather than in an artificial language like predicate logic, and we are using any kind of clear reasoning that shows that our conclusions follow from our premises, rather than restricting ourselves to mechanical rules of the sort that a simple computer program could check. But "informal" doesn't mean sloppy, and it doesn't mean that just anything goes. You may never have had to write out rigorous proofs before, and that's fine: this class does not assume that you already have these skills. You'll learn them.

Sometimes students say they don't know how to get started on an exercise. These techniques give you a way to get started. These are all pretty "low-level" techniques. With practice, they will become automatic, and when that happens you'll be able to give more of your attention to the really interesting parts of the proofs, instead of the basic details of "every" statements and "if" statements, and what is given and what you have to show. Once you get good at it, proving things can be like making music—but we have to start by practicing scales and arpeggios.

1 Give yourself room

It might be tempting to try to start writing down your proof from the beginning, and keep going until you reach the end. That doesn't usually work. The activity of **discovering** a proof and the activity of **presenting** or **explaining** a proof to others are very different. You're going to do both things, so to keep things clear you're going to need (at least) two pieces of paper: a *discovery* page, and a *presentation* page. Once you have discovered the whole proof, using the techniques we'll discuss, then you can write it down neatly from beginning to end. (See the section "Putting it together", sec. 6 below.)

2 Keep track of your goals

When you are working on a proof, you need to keep track of the answers to **the two most important questions.**

1. What am I trying to show?
2. What relevant things do I already know?

When you start working on your proof, start by writing down the answers to these questions. First write down "*Show*", and the statement of what you are trying to prove. Then write down "*Given*" (or "*Know*" or "*Assume" or "*Suppose*") and the statements of the things that you already know.

You shouldn't always try to write down *everything* you know. You can't always tell in advance what's going to be relevant, and you can always add something else to your list later when you think of it. But you should at least write down the things that are given to you in the statement of the exercise itself. You should also make sure to look carefully at the other definitions, lemmas, theorems, and exercises that come immediately before the exercise you're working on, and which use similar words or notation.

When you write these down, you should pay attention to the *logical structure* of each statement. Is it an "if … then …" statement? A "for all …" statement? A "there exists …" statement? There are different strategies to use for each of these kinds of statement, so it's important to figure out what kind you are dealing with.

As you go, your goals will change. (See the examples below.) You'll need to keep your notes organized so that you can easily tell what the answer is to the two key questions at your current stage of progress: What am I trying to show? What relevant things do I know?

3 Proving an "every" statement

Suppose this is your goal:

Show Every set is a subset of itself.

This is an "every" statement. We can rewrite it another way that makes its structure more explicit:

Show For every set A, A is a subset of A.

In this explicit form, an "every" statement has four parts.

1. "For every". This tells us what kind of statement we are dealing with—a *universal* statement, which says that *all* of a certain kind of thing have a certain property.

2. The *kind of thing* we are talking about: "set". (This is called the *restrictor*.)
3. The letter A; this is a *variable*. It doesn't matter very much which letter we use, but we'll want to choose a letter that isn't too confusing. There are conventions to use certain letters for certain kinds of things: for example, for *sets* we'll normally use the capital letters A, B, C, or X, Y, Z. We also want to avoid using a letter that we're already using for some other purpose. If we need to, we can add decorations to distinguish different variables from each other, like A', B_2, or $\hat{X}$.
4. The *property* we are showing that every set has—"A is a subset of A". (This is called the *matrix clause*.)

In English—even in the relatively regimented English of technical writing—"every" statements can come in a lot of forms. It's important to be able to recognize them, and to break them up into these four pieces. Here are some more examples (with brackets around the *restrictor* and the *matrix*).

3.1 Example

(a) All ravens are black.

For every [raven] x, [x is black].

(b) Any consistent set of sentences has a model.

For every [consistent set of sentences] X, [X has a model].

(c) If f is a function from A to B, then the range of f is a subset of B.

For every [function from A to B] f, [the range of f is a subset of B].

(d) Every closed term contains at least one constant.

For every [closed term] a, [a contains at least one constant].

(e) Every set is smaller than its power set.

For every [set] A, [A is smaller than A's power set].

(f) No set is as large as its own power set.

For every [set] A, [A is not as large as A's power set].

Now suppose we are trying to show an "every" statement, and we have identified its logical structure.

For every [set] A, [A is a subset of A].

Now here is our strategy:

Given	A is a set
Show	A is a subset of A

That is, we'll add "A is a set" to our list of "givens", and we'll write down "*Show* A is a subset of A." This doesn't solve the problem yet—but it *simplifies* the problem. Our problem asked us to prove something complex, with some logical structure. We have now broken down our goal into something *less* complex.

When we apply this strategy, it's important to be careful with our choice of variables. We can make mistakes if we have already been using the letter A for some other purpose that's different from showing this "for all" statement, if we mix them up.

Here's how this strategy works for our other example sentences.

3.2 Example

(a) All ravens are black.

Given	x is a raven
Show	x is black

(b) Any consistent set of sentences has a model.

Given	X is a consistent set of sentences
Show	X has a model

(c) If f is a function from A to B, then the range of f is a subset of B.

Given	f is a function from A to B
Show	The range of f is a subset of B

(d) Every closed term contains at least one constant.

Given	a is a closed term
Show	a contains at least one constant

(e) Every set is smaller than its power set.

Given	A is a set
Show	A is smaller than A's power set

(f) No set is as large as its own power set.

Given	A is a set
Show	A is not as large as A's power set

3.3 Exercise
Identify the logical structure of each of the following "every" statements, and use this structure to write down the new "given" and "to show" statements you would need to prove it.

(a) Every one-to-one correspondence is an onto function.

(b) Every set which is at least as large as the set of numbers is infinite.

(c) A set of sentences is logically consistent iff it has a model.

(d) For any sets A and B, if $A \subseteq B$ and $B \subseteq A$, then $A = B$.

(e) If A is any non-empty set, there is a one-to-one function A to B or there is an onto function from B to A, as long as A is not empty.

(f) No theory is simple, strong, consistent and complete.

4 Unpacking definitions

Suppose we have this goal:

Show	A is a subset of A.

This involves a technical term "subset", which has an official definition. We can look it up:

> **Definition.** If A and B are sets, then A is a **subset** of B iff every element of A is an element of B. This is also written $A \subseteq B$ for short. We say A is a **proper subset** of B iff A is a subset of B, but not the same set as B.

So we can use this definition to "unpack" our statement, transforming it into this:

Show	Every element of A is an element of A.

The same trick applies to technical *notation* which is expressed in symbols rather than words. The notation

$$A \subseteq A$$

is defined to be a shorthand for "A is a subset of A". So we can use the same definition to unpack this in exactly the same way, as "Every element of A is an element of A."

Notice that the particular *letters* used as variables in the definition don't matter. They are placeholders. We can plug in any sets we want. In this case, we have plugged the set A into *both* spots in the definition—both the "A" and the "B" slots from the definition get plugged up with A.

4.1 Example

We can use the definition above (of "subset" and "proper subset") to unpack the following statements.

(a) X is a proper subset of Y

Every element of X is an element of Y, and X and Y are not the same set.

(b) $B \subseteq A$

Every element of B is an element of A.

(Pay attention to the order!)

4.2 Example

Here are some more definitions.

- If A and B are sets, a function f from A to B is **one-to-one** iff for each $a, a' \in A$, if $fa = fa'$ then $a = a'$.
- If A and B are sets, A and B have the **same number of elements** iff there is a one-to-one correspondence between A and B. This is abbreviated $A \sim B$.
- A sentence A is a **logical truth** (or **valid**) iff A is true in every structure.

Here are some examples of how to unpack these definitions in different statements.

(a) There is a one-to-one function from A to its power set.

There is a function f from A to the power set of A such that, for each $a, a' \in A$, if $fa = fa'$, then $a = a'$.

(b) No set has the same number of elements as its power set.

There is no set X such that there is a one-to-one correspondence between X and the power set of X.

(Notice that in order to unpack the definition, we introduced a *variable* X for the set we are talking about. The letter X was arbitrary. We could have used A or B or A' or something else if we wanted to. We just want to be clear, and make sure that our choice doesn't conflict with other variables we are already using in the context of our proof.)

(c) The sentence `∀x(x = x)` is a logical truth.

The sentence `∀x(x = x)` is true in every structure.

(d) Every logical truth is a logical consequence of the empty set.

For every sentence A which is true in every structure, A is a logical consequence of the empty set.

4.3 Exercise

Unpack the definitions from above in the following statements.

(a) C is a logical truth.

(b) g is a one-to-one function from B to A.

(c) $\mathbb{N}$ (the set of all natural numbers) is not a subset of the empty set.

(d) The successor function suc (which is a function from $\mathbb{N}$ to $\mathbb{N}$) is one-to-one.

(e) The empty set is a proper subset of its power set.

(f) Every logical truth is consistent.

(g) There are one-to-one functions from A to B and from B to A.

(All of the examples we've discussed here are examples of what are called *explicit* definitions. Later on we'll encounter a different, trickier kind of definition, called an *inductive* definition.)

It can be tempting to try to unpack definitions as your very first line of attack on a problem. But usually this isn't a good idea. Notice that unlike most of our strategies, unpacking definitions turns *simple* statements into *more complicated* statements. That means that if you do it right away, you make your problem more complicated. Usually you want to wait to unpack definitions until *after* you've already applied all the other strategies you can (like the “proving an ‘every’ statement” technique). Sometimes you won’t have to unpack a definition at all to finish a problem. In those cases, your solution will be easier to discover and easier to understand if you keep the definition “packed in.”

5 Proving an “if” statement

Suppose we have this goal:

Show	If A is a subset of B, and B is a subset of C, then A is a subset of C.

The first thing to do is to identify its structure. In this case, we recognize that this is an “if … then …” statement. Other than the “if” and “then”, it has two parts:

> If [A is a subset of B, and B is a subset of C], then [A is a subset of C].

We can think of the first piece,

> A is a subset of B, and B is a subset of C

as the “input” for the “if … then …” statement, and we can think of the second piece

> A is a subset of C

as its “output.” What we want to show is that we can get *from* the input *to* the output. (These two pieces are called the *antecedent* and the *consequent*.) So here is our strategy:

Given	A is a subset of B, and B is a subset of C
Show	A is a subset of C.

That is, we can write down the first part in our list of “givens”, and write down “A is a subset of C” as our new “to show”.

While we’re at it, we can split up the “… and …” statement in our new “given”. We’re adding *two* assumptions:

Given	A is a subset of B
	B is a subset of C
Show	A is a subset of C

Now that we have new “givens” and a new “to show”, we can go on and apply more strategies to try to finish the proof. (“Unpacking definitions” is a good one to go for next.)

5.1 Example

Identify the “if … then …” structure of the following statements, and use this to write down the new “given” and “show” statements that you would use to prove them.

(a) If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

Given	$A \subseteq B$
	$B \subseteq A$
Show	$A = B$

(b) If there is an onto function from A to B, then there is a one-to-one function from B to A.

Given	There is an onto function from A to B
Show	There is a one-to-one function from B to A

(c) If there is a one-to-one function from A to B, then there is an onto function from B to A, unless A is empty.

Given	There is a one-to-one function from A to B
	A is not empty
Show	There is an onto function from B to A

(d) If $X \vDash A$ and $Y, A \vDash B$ then $X, Y \vDash B$

Given	$X \vDash A$
	$Y, A \vDash B$
Show	$X, Y \vDash B$

(Notice that you don’t even need to know what this notation means in order to identify the logical *structure*.)

5.2 Exercise

Identify the “if … then …” structure of the following statements, and use this to write down the new “given” and “show” statements that you would use to prove them.

(a) If A is no larger than B and B is no larger than C, then A is no larger than C.

(b) If $m \leq n$, then either $m = n$, or $\operatorname{suc} m \leq n$.

(c) If $\{A, B\}$ is consistent, then $\neg B$ is a logical consequence of A.

(d) If T is sufficiently strong, axiomatizable, and consistent, then T is incomplete.

6 Putting it together

6.1 Example

Suppose we are doing this exercise:

> Prove that every set is a subset of itself

We start by writing down our goal.

Show	Every set is a subset of itself

We don't have any relevant "givens" for this problem, but we will want to make sure to keep the definition of "subset" handy.

Our first step is to identify the structure of this statement. It looks like an "every" statement. Let's rewrite it so its logical structure is very clear.

Show	For every set A, A is a subset of A

Now we can break this up, given us a new goal:

Given	A is a set
Show	A is a subset of A

How can we solve this simpler problem? Our "given" and our "show" don't look like they have any more complex logical structure at this point, so it looks like it's time to unpack the definition of "subset."

Given	A is a set
Show	Every element of A is an element of A.

But now the thing we have to show is completely obvious. (You could break it down even further with the “every” strategy: *assume a* is an element of A, and then *show a* is an element of A—which is trivial. But there is no need to go this far in breaking it down.) So we’re done! That is, we’re done *discovering the structure* of our informal proof. The last step is to put together all of our pieces in the right order, to make the proof understandable to other people. Here is how this might go:

> Let A be a set. It is obvious that every element of A is an element of A. This means that A is a subset of A. So every set is a subset of itself.

This paragraph looks pretty different from the fragments that we wrote down on the way to finding it. Instead of a bunch of “givens” and “shows”, we have put the whole thing together in logical order, from beginning to end. The *order of discovery* is different from the *order of justification*. In the order of discovery, we wrote down whatever was going to be helpful for us at the time for our next stage of simplification. But in the order of justification, we want to write things down step-by-step, so that each part of the proof comes immediately *after* what it relies on for justification.

Roughly, the steps we took to *find* this proof correspond to the final structure of the *presented* proof, not from beginning to end, but rather from the outside in. We can represent the logical structure of our informal proof like this:

> [Let A be a set. [[It is obvious that] every element of A is an element of A. This means that] A is a subset of A.] So every set is a subset of itself.

The “highest” or “outermost” level of logical structure is the thing we were originally trying to prove:

> … So every set is a subset of itself.

The next level in corresponds to the first strategy we used to prove this, the “prove an “every” statement” strategy.

> Let A be a set. … A is a subset of A.

The next level in corresponds to the next strategy we used, unpacking the definition of “subset”

> … every element of A is an element of A. This means that …

And the final, deepest level corresponds to the last part of our process of discovery, where we noticed that the only thing thing we had left to show was obvious.

> … It is obvious that …

Here’s the basic idea. After you have found the logical structure of your proof, by breaking things down until your “Show” statement very obviously follows from your “Given” statement, you need to retrace your steps. It's helpful to start from the end, looking at the last statement of your proof—the main thing you are trying to show. Then ask "what strategy did I use to get to this point?" That tells you what should go *before* that step in your polished presentation of the proof. Keep doing this until the answer is "nothing—it was obvious". This will give you the *order* in which you need to write things down. As for the actual words you write down, there is no mechanical recipe. The goal is to communicate the steps of you proof in a way which is elegant, concise, accurate, and easy to understand. Getting there takes practice and a sense of style.

Let's look at another example.

6.2 Example

We have this goal:

Show	For any sets A, B, and C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

First we observe that this is an "every" statement. We can think of it as being built up out of three different nested "every" statements ("For every set A, for every set B, for every set C, …"). But it's simpler to just handle all three of them at once.

Given	A is a set B is a set C is a set
Show	If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$

Next we notice that we have an "if … then …" statement that we can break down. We'll keep our old "givens" and add some new ones.

Given	A is a set B is a set C is a set $A \subseteq B$ $B \subseteq C$
Show	$A \subseteq C$

This looks about as simple as we can get without unpacking definitions. So let's do that now. We'll unpack the definition of $\subseteq$ three times.

Given	A is a set
	B is a set
	C is a set
	Every element of A is an element of B
	Every element of B is an element of C
Show	Every element of A is an element of C

At this point we could declare it obvious enough that our "to show" follows from our "givens", and be done. But for the practice, let's go ahead and break this proof down into even more basic steps this time. Again, we have an "every" statement to show. We can restate it, introducing a new variable:

> For every [element of A] a, a is an element of C.

So we can break it down again:

Given	A is a set
	B is a set
	C is a set
	Every element of A is an element of B
	Every element of B is an element of C
	a is an element of A
Show	a is an element of C

And now it's clear how to finish. We know a is an element of A. One our assumptions tells us that this implies a is an element of B. Then another assumption tells us that *this* implies a is an element of C.

Now let's put this all together, and write up our informal proof.

> Let A, B, and C be sets, and suppose that $A \subseteq B$ and $B \subseteq C$. Let a be any element of A. Then since every element of A is an element of B, a is an element of B. And since every element of B is an element of C, a is an element of C. This shows that every element of A is an element of C. That is, $A \subseteq C$.

Once again, we can find the "order of discovery" here by looking at the proof from the outside in, more or less. At the outermost level, we find the traces of the "prove an 'every' " strategy and the "prove an 'if' " strategy that we began with.

> Let A, B, and C be sets, and suppose that $A \subseteq B$ and $B \subseteq C$. … $A \subseteq C$.

Looking a little bit further back from the end, we see a definition unpacked:

> … every element of A is an element of C. That is …

A bit further in yet, we have our second “every” strategy:

> Let a be any element of A. … a is an element of C. This shows that …

And at the middle of the proof we have our other two unpackings of the definition, and our final observation about how they are related.

> Then since every element of A is an element of B, a is an element of B. And since every element of B is an element of C, a is an element of C.

This is just a start. There are lots more strategies that we’ll discuss as we go. I’ll also add some of them to an updated version of this document. But this should be enough to get going on the exercises. You’ll also get lots more examples and lots more practice in the weeks to come.