3

Proofs

3.1. Proof Strategies

Mathematicians are skeptical people. They use many methods, including experimentation with examples, trial and error, and guesswork, to try to find answers to mathematical questions, but they are generally not convinced that an answer is correct unless they can prove it. You have probably seen some mathematical proofs before, but you may not have any experience writing them yourself. In this chapter you'll learn more about how proofs are put together, so you can start writing your own proofs.

Proofs are a lot like jigsaw puzzles. There are no rules about how jigsaw puzzles must be solved. The only rule concerns the final product: All the pieces must fit together, and the picture must look right. The same holds for proofs.

Although there are no rules about how jigsaw puzzles must be solved, some techniques for solving them work better than others. For example, you'd never do a jigsaw puzzle by filling in every *other* piece, and then going back and filling in the holes! But you also don't do it by starting at the top and filling in the pieces in order until you reach the bottom. You probably fill in the border first, and then gradually put other chunks of the puzzle together and figure out where they go. Sometimes you try to put pieces in the wrong places, realize that they don't fit, and feel that you're not making any progress. And every once in a while you see, in a satisfying flash, how two big chunks fit together and feel that you've suddenly made a lot of progress. As the pieces of the puzzle fall into place, a picture emerges. You suddenly realize that the patch of blue you've been putting together is a lake, or part of the sky. But it's only when the puzzle is complete that you can see the whole picture.

Similar things could be said about the process of figuring out a proof. And I think one more similarity should be mentioned. When you finish a jigsaw

puzzle, you don't take it apart right away, do you? You probably leave it out for a day or two, so you can admire it. You should do the same thing with a proof. You figured out how to fit it together yourself, and once it's all done, isn't it pretty?

In this chapter we will discuss the proof-writing techniques that mathematicians use most often and explain how to use them to begin writing proofs yourself. Understanding these techniques may also help you read and understand proofs written by other people. Unfortunately, the techniques in this chapter do not give a step-by-step procedure for solving every proof problem. When trying to write a proof you may make a few false starts before finding the right way to proceed, and some proofs may require some cleverness or insight. With practice your proof-writing skills should improve, and you'll be able to tackle more and more challenging proofs.

Mathematicians usually state the answer to a mathematical question in the form of a *theorem* that says that if certain assumptions called the *hypotheses* of the theorem are true, then some conclusion must also be true. Often the hypotheses and conclusion contain free variables, and in this case it is understood that these variables can stand for any elements of the universe of discourse. An assignment of particular values to these variables is called an *instance* of the theorem, and in order for the theorem to be correct it must be the case that for every instance of the theorem that makes the hypotheses come out true, the conclusion is also true. If there is even one instance in which the hypotheses are true but the conclusion is false, then the theorem is incorrect. Such an instance is called a *counterexample* to the theorem.

Example 3.1.1. Consider the following theorem:

Theorem. *Suppose* $x > 3$ *and* $y < 2$. *Then* $x^2 - 2y > 5$.

This theorem is correct. (You are asked to prove it in exercise 14.) The hypotheses of the theorem are $x > 3$ and $y < 2$, and the conclusion is $x^2 - 2y > 5$. As an instance of the theorem, we could plug in 5 for x and 1 for y. Clearly with these values of the variables the hypotheses $x > 3$ and $y < 2$ are both true, so the theorem tells us that the conclusion $x^2 - 2y > 5$ must also be true. In fact, plugging in the values of x and y we find that $x^2 - 2y = 25 - 2 = 23$, and certainly $23 > 5$. Note that this calculation does not constitute a proof of the theorem. We have only checked one instance of the theorem, and a proof would have to show that *all* instances are correct.

If we drop the second hypothesis, then we get an incorrect theorem:

Incorrect Theorem. *Suppose* $x > 3$. *Then* $x^2 - 2y > 5$.

We can see that this theorem is incorrect by finding a counterexample. For example, suppose we let $x = 4$ and $y = 6$. Then the only remaining hypothesis, $x > 3$, is true, but $x^2 - 2y = 16 - 12 = 4$, so the conclusion $x^2 - 2y > 5$ is false.

If you find a counterexample to a theorem, then you can be sure that the theorem is incorrect, but the only way to know for sure that a theorem is correct is to prove it. A proof of a theorem is simply a deductive argument whose premises are the hypotheses of the theorem and whose conclusion is the conclusion of the theorem. Of course the argument should be valid, so we can be sure that if the hypotheses of the theorem are true, then the conclusion must be true as well. How you figure out and write up the proof of a theorem will depend mostly on the logical form of the conclusion. Often it will also depend on the logical forms of the hypotheses. The proof-writing techniques we will discuss in this chapter will tell you which proof strategies are most likely to work for various forms of hypotheses and conclusions.

Proof-writing techniques that are based on the logical forms of the hypotheses usually suggest ways of drawing inferences from the hypotheses. When you draw an inference from the hypotheses, you use the assumption that the hypotheses are true to justify the assertion that some other statement is also true. Once you have shown that a statement is true, you can use it later in the proof exactly as if it were a hypothesis. Perhaps the most important rule to keep in mind when drawing such inferences is this: *Never assert anything until you can justify it completely* using the hypotheses or using conclusions reached from them earlier in the proof. Your motto should be: "I shall make no assertion before its time." Following this rule will prevent you from using circular reasoning or jumping to conclusions and will guarantee that, if the hypotheses are true, then the conclusion must also be true. And this is the primary purpose of any proof: to provide a guarantee that the conclusion is true if the hypotheses are.

To make sure your assertions are adequately justified, you must be skeptical about every inference in your proof. If there is any doubt in your mind about whether the justification you have given for an assertion is adequate, then it isn't. After all, if your own reasoning doesn't even convince *you*, how can you expect it to convince anybody else?

Proof-writing techniques based on the logical form of the conclusion are often somewhat different from techniques based on the forms of the hypotheses. They usually suggest ways of transforming the problem into one that is equivalent but easier to solve. The idea of solving a problem by transforming it into an easier problem should be familiar to you. For example, adding the same

number to both sides of an equation transforms the equation into an equivalent equation, and the resulting equation is sometimes easier to solve than the original one. Students who have studied calculus may be familiar with techniques of evaluating integrals, such as substitution or integration by parts, that can be used to transform a difficult integration problem into an easier one.

Proofs that are written using these transformation strategies often include steps in which you assume for the sake of argument that some statement is true without providing any justification for that assumption. It may seem at first that such reasoning would violate the rule that assertions must always be justified, but it doesn't, because *assuming* something is not the same as *asserting* it. To assert a statement is to claim that it is true, and such a claim is never acceptable in a proof unless it can be justified. However, the purpose of making an assumption in a proof is not to make a claim about what *is* true, but rather to enable you to find out what *would be* true *if* the assumption were correct. You must always keep in mind that any conclusion you reach that is based on an assumption might turn out to be false if the assumption is incorrect. Whenever you make a statement in a proof, it's important to be sure you know whether it's an assertion or an assumption.

Perhaps an example will help clarify this. Suppose during the course of a proof you decide to assume that some statement, call it P, is true, and you use this assumption to conclude that another statement Q is true. It would be wrong to call this a proof that Q is true, because you can't be sure that your assumption about the truth of P was correct. All you can conclude at this point is that *if* P is true, then you can be sure that Q is true as well. In other words, you know that the statement $P \to Q$ is true. If the conclusion of the theorem being proven was Q, then the proof is incomplete at best. But if the conclusion was $P \to Q$, then the proof is complete. This brings us to our first proof strategy.

To prove a conclusion of the form $P \to Q$:
Assume P is true and then prove Q.

Here's another way of looking at what this proof technique means. Assuming that P is true amounts to the same thing as adding P to your list of hypotheses. Although P might not originally have been one of your hypotheses, once you have assumed it, you can use it exactly the way you would use any other hypothesis. Proving Q means treating Q as your conclusion and forgetting about the original conclusion. So this technique says that if the conclusion of the theorem you are trying to prove has the form $P \to Q$, then you can *transform the problem* by adding P to your list of hypotheses and

changing your conclusion from $P \to Q$ to Q. This gives you a new, perhaps easier proof problem to work on. If you can solve the new problem, then you will have shown that *if* P is true then Q is also true, thus solving the original problem of proving $P \to Q$. How you solve this new problem will now be guided by the logical form of the new conclusion Q (which might itself be a complex statement), and perhaps also by the logical form of the new hypothesis P.

Note that this technique doesn't tell you how to do the whole proof, it just gives you one step, leaving you with a new problem to solve in order to finish the proof. Proofs are usually not written all at once, but are created gradually by applying several proof techniques one after another. Often the use of these techniques will lead you to transform the problem several times. In discussing this process it will be helpful to have some way to keep track of the results of this sequence of transformations. We therefore introduce the following terminology. We will refer to the statements that are known or assumed to be true at some point in the course of figuring out a proof as *givens*, and the statement that remains to be proven at that point as the *goal*. When you are starting to figure out a proof, the givens will be just the hypotheses of the theorem you are proving, but they may later include other statements that have been inferred from the hypotheses or added as new assumptions as the result of some transformation of the problem. The goal will initially be the conclusion of the theorem, but it may be changed several times in the course of figuring out a proof.

To keep in mind that all of our proof strategies apply not only to the original proof problem but also to the results of any transformation of the problem, we will talk from now on only about givens and goals, rather than hypotheses and conclusions, when discussing proof-writing strategies. For example, the strategy stated earlier should really be called a strategy for proving a *goal* of the form $P \to Q$, rather than a conclusion of this form. Even if the conclusion of the theorem you are proving is not a conditional statement, if you transform the problem in such a way that a conditional statement becomes the goal, then you can apply this strategy as the next step in figuring out the proof.

Example 3.1.2. Suppose a and b are real numbers. Prove that if $0 < a < b$ then $a^2 < b^2$.

Scratch work

We are given as a hypothesis that a and b are real numbers. Our conclusion has the form $P \to Q$, where P is the statement $0 < a < b$ and Q is the statement

$a^2 < b^2$. Thus we start with these statements as given and goal:

Givens	*Goal*
a and b are real numbers	$(0 < a < b) \to (a^2 < b^2)$

According to our proof technique we should assume that $0 < a < b$ and try to use this assumption to prove that $a^2 < b^2$. In other words, we transform the problem by adding $0 < a < b$ to the list of givens and making $a^2 < b^2$ our goal:

Givens	*Goal*
a and b are real numbers	$a^2 < b^2$
$0 < a < b$	

Comparing the inequalities $a < b$ and $a^2 < b^2$ suggests that multiplying both sides of the given inequality $a < b$ by either a or b might get us closer to our goal. Because we are given that a and b are positive, we won't need to reverse the direction of the inequality if we do this. Multiplying $a < b$ by a gives us $a^2 < ab$, and multiplying it by b gives us $ab < b^2$. Thus $a^2 < ab < b^2$, so $a^2 < b^2$.

Solution

Theorem. *Suppose a and b are real numbers. If* $0 < a < b$ *then* $a^2 < b^2$.
Proof. Suppose $0 < a < b$. Multiplying the inequality $a < b$ by the positive number a we can conclude that $a^2 < ab$, and similarly multiplying by b we get $ab < b^2$. Therefore $a^2 < ab < b^2$, so $a^2 < b^2$, as required. Thus, if $0 < a < b$ then $a^2 < b^2$. □

As you can see from the preceding example, there's a difference between the reasoning you use when you are figuring out a proof and the steps you write down when you write the final version of the proof. In particular, although we will often talk about givens and goals when trying to figure out a proof, the final write-up will rarely refer to them. Throughout this chapter, and sometimes in later chapters as well, we will precede our proofs with the scratch work used to figure out the proof, but this is just to help you understand how proofs are constructed. When mathematicians write proofs, they usually just write the steps needed to justify their conclusions with no explanation of how they thought of them. Some of these steps will be sentences indicating that the problem has been transformed (usually according to some proof strategy based on the logical form of the goal); some steps will be assertions that are justified by inferences from the givens (often using some proof strategy based on the logical form of a given). However, there

will usually be no explanation of how the mathematician thought of these transformations and inferences. For example, the proof in Example 3.1.2 starts with the sentence "Suppose $0 < a < b$," indicating that the problem has been transformed according to our strategy, and then proceeds with a sequence of inferences leading to the conclusion that $a^2 < b^2$. No other explanations were necessary to justify the final conclusion, in the last sentence, that if $0 < a < b$ then $a^2 < b^2$.

Although this lack of explanation sometimes makes proofs hard to read, it serves the purpose of keeping two distinct objectives separate: *explaining your thought processes* and *justifying your conclusions*. The first is psychology; the second, mathematics. The primary purpose of a proof is to justify the claim that the conclusion follows from the hypotheses, and no explanation of your thought processes can substitute for adequate justification of this claim. Keeping any discussion of thought processes to a minimum in a proof helps to keep this distinction clear. Occasionally, in a very complicated proof, a mathematician may include some discussion of the strategy behind the proof to make the proof easier to read. Usually, however, it is up to readers to figure this out for themselves. Don't worry if you don't immediately understand the strategy behind a proof you are reading. Just try to follow the justifications of the steps, and the strategy will eventually become clear. If it doesn't, a second reading of the proof might help.

To keep the distinction between the proof and the strategy behind the proof clear, in the future when we state a proof strategy we will often describe both the scratch work you might use to figure out the proof and the form that the final write-up of the proof should take. For example, here's a restatement of the proof strategy we discussed earlier, in the form we will be using to present proof strategies from now on.

To prove a goal of the form $P \to Q$:
Assume P is true and then prove Q.

Scratch work

Before using strategy:

Givens	*Goal*
—	$P \to Q$
—	

After using strategy:

Givens	*Goal*
—	Q
—	
P	

Form of final proof:

Suppose P.
  [Proof of Q goes here.]
Therefore $P \to Q$.

Note that the suggested form for the final proof tells you how the beginning and end of the proof will go, but more steps will have to be added in the middle. The givens and goal list under the heading "After using strategy" tells you what is known or can be assumed and what needs to be proven in order to fill in this gap in the proof. Many of our proof strategies will tell you how to write either the beginning or the end of your proof, leaving a gap to be filled in with further reasoning.

There is a second method that is sometimes used for proving goals of the form $P \to Q$. Because any conditional statement $P \to Q$ is equivalent to its contrapositive $\neg Q \to \neg P$, you can prove $P \to Q$ by proving $\neg Q \to \neg P$ instead, using the strategy discussed earlier. In other words:

To prove a goal of the form $P \to Q$:
  Assume Q is false and prove that P is false.

Scratch work

Before using strategy:

Givens	*Goal*
—	$P \to Q$
—	

After using strategy:

Givens	*Goal*
—	$\neg P$
—	
$\neg Q$	

Form of final proof:

Suppose Q is false.
  [Proof of $\neg P$ goes here.]
Therefore $P \to Q$.

Example 3.1.3. Suppose *a, b,* and c are real numbers and $a > b$. Prove that if $ac \leq bc$ then $c \leq 0$.

Scratch work

Givens	*Goal*
a, b, and c are real numbers	$(ac \leq bc) \to (c \leq 0)$
$a > b$	

The contrapositive of the goal is $\neg(c \leq 0) \to \neg(ac \leq bc)$, or in other words $(c > 0) \to (ac > bc)$, so we can prove it by adding $c > 0$ to the list of givens and making $ac > bc$ our new goal:

Givens	*Goal*
a, b, and c are real numbers	$ac > bc$
$a > b$	
$c > 0$	

We can also now write the first and last sentences of the proof. According to the strategy, the final proof should have this form:

> Suppose $c > 0$.
>
> [Proof of $ac > bc$ goes here.]
>
> Therefore, if $ac \leq bc$ then $c \leq 0$.

Using the new given $c > 0$, we see that the goal $ac > bc$ follows immediately from the given $a > b$ by multiplying both sides by the positive number c. Inserting this step between the first and last sentences completes the proof.

Solution

Theorem. *Suppose a, b, and c are real numbers and $a > b$. If $ac \leq bc$ then $c \leq 0$.*

Proof. We will prove the contrapositive. Suppose $c > 0$. Then we can multiply both sides of the given inequality $a > b$ by c and conclude that $ac > bc$. Therefore, if $ac \leq bc$ then $c \leq 0$. □

Notice that, although we have used the symbols of logic freely in the scratch work, we have not used them in the final write-up of the proof. Although it would not be incorrect to use logical symbols in a proof, mathematicians usually try to avoid it. Using the notation and rules of logic can be very helpful when you are figuring out the strategy for a proof, but in the final write-up you should try to stick to ordinary English as much as possible.

The reader may be wondering how we knew in Example 3.1.3 that we should use the second method for proving a goal of the form $P \to Q$

rather than the first. The answer is simple: We tried both methods, and the second worked. When there is more than one strategy for proving a goal of a particular form, you may have to try a few different strategies before you hit on one that works. With practice, you will get better at guessing which strategy is most likely to work for a particular proof.

Notice that in each of the examples we have given our strategy involved making changes in our givens and goal to try to make the problem easier. The beginning and end of the proof, which were supplied for us in the statement of the proof technique, serve to tell a reader of the proof that these changes have been made and how the solution to this revised problem solves the original problem. The rest of the proof contains the solution to this easier, revised problem.

Most of the other proof techniques in this chapter also suggest that you revise your givens and goal in some way. These revisions result in a new proof problem, and in every case the revisions have been designed so that a solution to the new problem, when combined with some beginning or ending sentences explaining these revisions, would also solve the original problem. This means that whenever you use one of these strategies you can write a sentence or two at the beginning or end of the proof and then forget about the original problem and work instead on the new problem, which will usually be easier. Often you will be able to figure out a proof by using the techniques in this chapter to revise your givens and goal repeatedly, making the remaining problem easier and easier until you reach a point at which it is completely obvious that the goal follows from the givens.

Exercises

*1. Consider the following theorem. (This theorem was proven in the introduction.)

Theorem. *Suppose n is an integer larger than 1 and n is not prime. Then* $2^n - 1$ *is not prime.*

(a) Identify the hypotheses and conclusion of the theorem. Are the hypotheses true when $n = 6$? What does the theorem tell you in this instance? Is it right?
(b) What can you conclude from the theorem in the case $n = 15$? Check directly that this conclusion is correct.
(c) What can you conclude from the theorem in the case $n = 11$?

2. Consider the following theorem. (The theorem is correct, but we will not ask you to prove it here.)