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 $P \rightarrow Q$ is true. If the conclusion of the theorem being proven was Q, then the proof is incomplete at best. But if the conclusion was $P \rightarrow Q$, then the proof is complete. This brings us to our first proof strategy.

To prove a conclusion of the form $P \rightarrow Q$:
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 $P \rightarrow Q$, then you can *transform the problem* by adding P to your list of hypotheses and changing your conclusion from $P \rightarrow Q$ 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 $P \rightarrow Q$. 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 $P \rightarrow Q$, 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 $P \rightarrow Q$, 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	$(0 < a < b) \rightarrow (a^2 < b^2)$

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 $P \rightarrow Q$.

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 $P \rightarrow Q$. Because any conditional statement $P \rightarrow Q$ is equivalent to its contrapositive $\neg Q \rightarrow \neg P$, you can prove $P \rightarrow Q$ by proving $\neg Q \rightarrow \neg P$ instead, using the strategy discussed earlier. In other words:

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

Scratch work

Before using strategy:

Givens	*Goal*
—	$P \rightarrow Q$
—	

After using strategy:

Givens	*Goal*
—	$\neg P$
—	
$\neg Q$	

Form of final proof:

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

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	$(ac \leq bc) \rightarrow (c \leq 0)$
$a > b$	

The contrapositive of the goal is $\neg(c \leq 0) \rightarrow \neg(ac \leq bc)$, or in other words $(c > 0) \rightarrow (ac > bc)$, 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 $P \rightarrow Q$

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.)

Theorem. *Suppose that $b^2 > 4ac$. Then the quadratic equation $ax^2 + bx + c = 0$ has exactly two real solutions.*

(a) Identify the hypotheses and conclusion of the theorem.
(b) To give an instance of the theorem, you must specify values for a, b, and c, but not x. Why?
(c) What can you conclude from the theorem in the case $a = 2$, $b = -5$, $c = 3$? Check directly that this conclusion is correct.
(d) What can you conclude from the theorem in the case $a = 2$, $b = 4$, $c = 3$?

3. Consider the following incorrect theorem:

Incorrect Theorem. *Suppose n is a natural number larger than 2, and n is not a prime number. Then 2n + 13 is not a prime number.*

What are the hypotheses and conclusion of this theorem? Show that the theorem is incorrect by finding a counterexample.

*4. Complete the following alternative proof of the theorem in Example 3.1.2.

Proof. Suppose $0 < a < b$. Then $b - a > 0$.
[Fill in a proof of $b^2 - a^2 > 0$ here.]
Since $b^2 - a^2 > 0$, it follows that $a^2 < b^2$. Therefore if $0 < a < b$ then $a^2 < b^2$. □

5. Suppose a and b are real numbers. Prove that if $a < b < 0$ then $a^2 > b^2$.
6. Suppose a and b are real numbers. Prove that if $0 < a < b$ then $1/b < 1/a$.
7. Suppose that a is a real number. Prove that if $a^3 > a$ then $a^5 > a$. (Hint: One approach is to start by completing the following equation: $a^5 - a = (a^3 - a) \cdot \underline{\ ?\ }$.)
8. Suppose $A \setminus B \subseteq C \cap D$ and $x \in A$. Prove that if $x \notin D$ then $x \in B$.
*9. Suppose a and b are real numbers. Prove that if $a < b$ then $\frac{a+b}{2} < b$.
10. Suppose x is a real number and $x \neq 0$. Prove that if $\frac{\sqrt[3]{x}+5}{x^2+6} = \frac{1}{x}$ then $x \neq 8$.
*11. Suppose a, b, c, and d are real numbers, $0 < a < b$, and $d > 0$. Prove that if $ac \geq bd$ then $c > d$.
12. Suppose x and y are real numbers, and $3x + 2y \leq 5$. Prove that if $x > 1$ then $y < 1$.
13. Suppose that x and y are real numbers. Prove that if $x^2 + y = -3$ and $2x - y = 2$ then $x = -1$.

*14. Prove the first theorem in Example 3.1.1. (Hint: You might find it useful to apply the theorem from Example 3.1.2.)

15. Consider the following theorem.

 Theorem. *Suppose x is a real number and $x \neq 4$. If $\frac{2x-5}{x-4} = 3$ then $x = 7$.*

 (a) What's wrong with the following proof of the theorem?

 Proof. Suppose $x = 7$. Then $\frac{2x-5}{x-4} = \frac{2(7)-5}{7-4} = \frac{9}{3} = 3$. Therefore if $\frac{2x-5}{x-4} = 3$ then $x = 7$. □

 (b) Give a correct proof of the theorem.

16. Consider the following incorrect theorem:

 Incorrect Theorem. *Suppose that x and y are real numbers and $x \neq 3$. If $x^2y = 9y$ then $y = 0$.*

 (a) What's wrong with the following proof of the theorem?

 Proof. Suppose that $x^2y = 9y$. Then $(x^2 - 9)y = 0$. Since $x \neq 3$, $x^2 \neq 9$, so $x^2 - 9 \neq 0$. Therefore we can divide both sides of the equation $(x^2 - 9)y = 0$ by $x^2 - 9$, which leads to the conclusion that $y = 0$. Thus, if $x^2y = 9y$ then $y = 0$. □

 (b) Show that the theorem is incorrect by finding a counterexample.

3.2. Proofs Involving Negations and Conditionals

We turn now to proofs in which the goal has the form $\neg P$. Usually it's easier to prove a positive than a negative statement, so it is often helpful to reexpress a goal of the form $\neg P$ before proving it. Instead of using a goal that says what *shouldn't* be true, see if you can rephrase it as a goal that says what *should* be true. Fortunately, we have already studied several equivalences that will help with this reexpression. Thus, our first strategy for proving negated statements is:

To prove a goal of the form $\neg P$:

If possible, reexpress the goal in some other form and then use one of the proof strategies for this other goal form.

Example 3.2.1. Suppose $A \cap C \subseteq B$ and $a \in C$. Prove that $a \notin A \setminus B$.

Scratch Work

Givens	*Goal*
$A \cap C \subseteq B$	$a \notin A \setminus B$
$a \in C$	

Because the goal is a negated statement, we try to reexpress it:

$$
\begin{aligned}
a \notin A \setminus B \text{ is equivalent to } &\neg(a \in A \wedge a \notin B) && \text{(definition of } A \setminus B\text{)},\\
\text{which is equivalent to } &a \notin A \vee a \in B && \text{(DeMorgan's law)},\\
\text{which is equivalent to } &a \in A \rightarrow a \in B && \text{(conditional law)}.
\end{aligned}
$$

Rewriting the goal in this way gives us:

Givens	*Goal*
$A \cap C \subseteq B$	$a \in A \rightarrow a \in B$
$a \in C$	

We now prove the goal in this new form, using the first strategy from Section 3.1. Thus, we add $a \in A$ to our list of givens and make $a \in B$ our goal:

Givens	*Goal*
$A \cap C \subseteq B$	$a \in B$
$a \in C$	
$a \in A$	

The proof is now easy: From the givens $a \in A$ and $a \in C$ we can conclude that $a \in A \cap C$, and then, since $A \cap C \subseteq B$, it follows that $a \in B$.

Solution

Theorem. *Suppose $A \cap C \subseteq B$ and $a \in C$. Then $a \notin A \setminus B$.*
Proof. Suppose $a \in A$. Then since $a \in C$, $a \in A \cap C$. But then since $A \cap C \subseteq B$ it follows that $a \in B$. Thus, it cannot be the case that a is an element of A but not B, so $a \notin A \setminus B$. □

Sometimes a goal of the form $\neg P$ cannot be reexpressed as a positive statement, and therefore this strategy cannot be used. In this case it is usually best to do a *proof by contradiction*. Start by assuming that P is true, and try to use this assumption to prove something that you know is false. Often this is done by proving a statement that contradicts one of the givens. Because you know that the statement you have proven is false, the assumption that P was true must have been incorrect. The only remaining possibility then is that P is false.

To prove a goal of the form $\neg P$:

Assume P is true and try to reach a contradiction. Once you have reached a contradiction, you can conclude that P must be false.

Scratch work

Before using strategy:

Givens	*Goal*
—	$\neg P$
—	

After using strategy:

Givens	*Goal*
—	Contradiction
—	
P	

Form of final proof:

> Suppose P is true.
> [Proof of contradiction goes here.]
> Thus, P is false.

Example 3.2.2. Prove that if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Scratch work

The goal is a conditional statement, so according to the first proof strategy in Section 3.1 we can treat the antecedent as given and make the consequent our new goal:

Givens	*Goal*
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

This proof strategy also suggests what form the final proof should take. According to the strategy, the proof should look like this:

> Suppose $x^2 + y = 13$ and $y \neq 4$.
> [Proof of $x \neq 3$ goes here.]
> Thus, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

In other words, the first and last sentences of the final proof have already been written, and the problem that remains to be solved is to fill in a proof of $x \neq 3$

between these two sentences. The givens–goal list summarizes what we know and what we have to prove in order to solve this problem.

The goal $x \neq 3$ means $\neg(x = 3)$, but because $x = 3$ has no logical connectives in it, none of the equivalences we know can be used to reexpress this goal in a positive form. We therefore try proof by contradiction and transform the problem as follows:

Givens	*Goal*
$x^2 + y = 13$	Contradiction
$y \neq 4$	
$x = 3$	

Once again, the proof strategy that suggested this transformation also tells us how to fill in a few more sentences of the final proof. As we indicated earlier, these sentences go between the first and last sentences of the proof, which were written before.

Suppose $x^2 + y = 13$ and $y \neq 4$.
  Suppose $x = 3$.
    [Proof of contradiction goes here.]
  Therefore $x \neq 3$.
Thus, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

The indenting in this outline of the proof will not be part of the final proof. We have done it here to make the underlying structure of the proof clear. The first and last lines go together and indicate that we are proving a conditional statement by assuming the antecedent and proving the consequent. Between these lines is a proof of the consequent, $x \neq 3$, which we have set off from the first and last lines by indenting it. This inner proof has the form of a proof by contradiction, as indicated by its first and last lines. Between these lines we still need to fill in a proof of a contradiction.

At this point we don't have a particular statement as our goal; any impossible conclusion will do. We must therefore look more closely at the givens to see if some of them contradict others. In this case, the first and third together imply that $y = 4$, which contradicts the second.

Solution

Theorem. *If* $x^2 + y = 13$ *and* $y \neq 4$ *then* $x \neq 3$.

Proof. Suppose $x^2 + y = 13$ and $y \neq 4$. Suppose $x = 3$. Substituting this into the equation $x^2 + y = 13$, we get $9 + y = 13$, so $y = 4$. But this contradicts the fact that $y \neq 4$. Therefore $x \neq 3$. Thus, if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$. □

You may be wondering at this point why we were justified in concluding, when we reached a contradiction in the proof, that $x \neq 3$. After all, the second list of givens in our scratch work contained three given. How could we be sure, when we reached a contradiction, that the culprit was the third given, $x = 3$? To answer this question, look back at the first givens and goal analysis for this example. According to that analysis, there were two givens, $x^2 + y = 13$ and $y \neq 4$, from which we had to prove the goal $x \neq 3$. Remember that a proof only has to guarantee that the goal is true *if* the givens are. Thus, we didn't have to show that $x \neq 3$, only that *if* $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$. When we reached a contradiction, we knew that one of the three statements in the second list of givens had to be false. We didn't try to figure out which one it was because we didn't need to. We were certainly justified in concluding that *if* neither of the first two was the culprit, then it had to be the third, and that was all that was required to finish the proof.

Proving a goal by contradiction has the advantage that it allows you to assume that your conclusion is false, providing you with another given to work with. But it has the disadvantage that it leaves you with a rather vague goal: produce a contradiction by proving something that you know is false. Because all the proof strategies we have discussed so far depend on analyzing the logical form of the goal, it appears that none of them will help you to achieve the goal of producing a contradiction. In the preceding proof we were forced to look more closely at our givens to find a contradiction. In this case we did it by proving that $y = 4$, contradicting the given $y \neq 4$. This illustrates a pattern that occurs often in proofs by contradiction: If one of the givens has the form $\neg P$, then you can produce a contradiction by proving P. This is our first strategy based on the logical form of a *given*.

To use a given of the form $\neg P$:

If you're doing a proof by contradiction, try making P your goal. If you can prove P, then the proof will be complete, because P contradicts the given $\neg P$.

Scratch work

Before using strategy:

Givens	*Goal*
$\neg P$	Contradiction
—	
—	

After using strategy:

Givens	*Goal*
$\neg P$	P
—	
—	

Form of final proof:

[Proof of P goes here.]
Since we already know $\neg P$, this is a contradiction.

Although we have recommended proof by contradiction for proving goals of the form $\neg P$, it can be used for any goal. Usually it's best to try the other strategies first if any of them apply; but if you're stuck, you can try proof by contradiction in any proof.

The next example illustrates this and also another important rule of proof-writing: In many cases the logical form of a statement can be discovered by *writing out the definition* of some mathematical word or symbol that occurs in the statement. For this reason, knowing the precise statements of the definitions of all mathematical terms is extremely important when you're writing a proof.

Example 3.2.3. Suppose A, B, and C are sets, $A \setminus B \subseteq C$, and x is anything at all. Prove that if $x \in A \setminus C$ then $x \in B$.

Scratch work

We're given that $A \setminus B \subseteq C$, and our goal is $x \in A \setminus C \rightarrow x \in B$. Because the goal is a conditional statement, our first step is to transform the problem by adding $x \in A \setminus C$ as a second given and making $x \in B$ our goal:

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in B$
$x \in A \setminus C$	

The form of the final proof will therefore be as follows:

Suppose $x \in A \setminus C$.
[Proof of $x \in B$ goes here.]
Thus, if $x \in A \setminus C$ then $x \in B$.

The goal $x \in B$ contains no logical connectives, so none of the techniques we have studied so far apply, and it is not obvious why the goal follows from the givens. Lacking anything else to do, we try proof by contradiction:

Givens	*Goal*
$A \setminus B \subseteq C$	Contradiction
$x \in A \setminus C$	
$x \notin B$	

As before, this transformation of the problem also enables us to fill in a few more sentences of the proof:

> Suppose $x \in A \setminus C$.
>   Suppose $x \notin B$.
>   [Proof of contradiction goes here.]
>   Therefore $x \in B$.
> Thus, if $x \in A \setminus C$ then $x \in B$.

Because we're doing a proof by contradiction and our last given is now a negated statement, we could try using our strategy for using givens of the form $\neg P$. Unfortunately, this strategy suggests making $x \in B$ our goal, which just gets us back to where we started. We must look at the other givens to try to find the contradiction.

In this case, writing out the definition of the second given is the key to the proof, since this definition also contains a negated statement. By definition, $x \in A \setminus C$ means $x \in A$ and $x \notin C$. Replacing this given by its definition gives us:

Givens	*Goal*
$A \setminus B \subseteq C$	Contradiction
$x \in A$	
$x \notin C$	
$x \notin B$	

Now the third given also has the form $\neg P$, where P is the statement $x \in C$, so we can apply the strategy for using givens of the form $\neg P$ and make $x \in C$ our goal. Showing that $x \in C$ would complete the proof because it would contradict the given $x \notin C$.

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in C$
$x \in A$	
$x \notin C$	
$x \notin B$	

Once again, we can add a little more to the proof we are gradually writing by filling in the fact that we plan to derive our contradiction by proving $x \in C$.

We also add the definition of $x \in A \setminus C$ to the proof, inserting it in what seems like the most logical place, right after we stated that $x \in A \setminus C$:

> Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$.
> Suppose $x \notin B$.
> [Proof of $x \in C$ goes here.]
> This contradicts the fact that $x \notin C$.
> Therefore $x \in B$.
> Thus, if $x \in A \setminus C$ then $x \in B$.

We have finally reached a point where the goal follows easily from the givens. From $x \in A$ and $x \notin B$ we conclude that $x \in A \setminus B$. Since $A \setminus B \subseteq C$ it follows that $x \in C$.

Solution

Theorem. *Suppose A, B, and C are sets, $A \setminus B \subseteq C$, and x is anything at all. If $x \in A \setminus C$ then $x \in B$.*
Proof. Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$. Then $x \in A \setminus B$, so since $A \setminus B \subseteq C$, $x \in C$. But this contradicts the fact that $x \notin C$. Therefore $x \in B$. Thus, if $x \in A \setminus C$ then $x \in B$. □

The strategy we've recommended for using givens of the form $\neg P$ only applies if you are doing a proof by contradiction. For other kinds of proofs, the next strategy can be used. This strategy is based on the fact that givens of the form $\neg P$, like goals of this form, may be easier to work with if they are reexpressed as positive statements.

To use a given of the form $\neg P$:
If possible, reexpress this given in some other form.

We have discussed strategies for working with both givens and goals of the form $\neg P$, but only strategies for goals of the form $P \rightarrow Q$. We now fill this gap by giving two strategies for using givens of the form $P \rightarrow Q$. We said before that many strategies for using givens suggest ways of drawing inferences from the givens. Such strategies are called *rules of inference*. Both of our strategies for using givens of the form $P \rightarrow Q$ are examples of rules of inference.

To use a given of the form $P \rightarrow Q$:
If you are also given P, or if you can prove that P is true, then you can use this given to conclude that Q is true. Since it is equivalent to $\neg Q \rightarrow \neg P$,

if you can prove that Q is false, you can use this given to conclude that P is false.

The first of these rules of inference says that if you know that both P and $P \rightarrow Q$ are true, you can conclude that Q must also be true. Logicians call this rule *modus ponens*. We saw this rule used in one of our first examples of valid deductive reasoning in Chapter 1, argument 2 in Example 1.1.1. The validity of this form of reasoning was verified using the truth table for the conditional connective in Section 1.5.

The second rule, called *modus tollens*, says that if you know that $P \rightarrow Q$ is true and Q is false, you can conclude that P must also be false. The validity of this rule can also be checked with truth tables, as you are asked to show in exercise 13. Usually you won't find a given of the form $P \rightarrow Q$ to be much use until you are able to prove either P or $\neg Q$. However, if you ever reach a point in your proof where you have determined that P is true, you should probably use this given immediately to conclude that Q is true. Similarly, if you ever establish $\neg Q$, immediately use this given to conclude $\neg P$.

Although most of our examples will involve specific mathematical statements, occasionally we will do examples of proofs containing letters standing for unspecified statements. Later in this chapter we will be able to use this method to verify some of the equivalences from Chapter 2 that could only be justified on intuitive grounds before. Here's an example of this kind, illustrating the use of modus ponens and modus tollens.

Example 3.2.4. Suppose $P \rightarrow (Q \rightarrow R)$. Prove that $\neg R \rightarrow (P \rightarrow \neg Q)$.

Scratch work

This could actually be done with a truth table, as you are asked to show in exercise 14, but let's do it using the proof strategies we've been discussing. We start with the following situation:

Givens	*Goal*
$P \rightarrow (Q \rightarrow R)$	$\neg R \rightarrow (P \rightarrow \neg Q)$

Our only given is a conditional statement. By the rules of inference just discussed, if we knew P we could use modus ponens to conclude $Q \rightarrow R$, and if we knew $\neg(Q \rightarrow R)$ we could use modus tollens to conclude $\neg P$. Because we don't, at this point, know either of these, we can't yet do anything with this given. If either P or $\neg(Q \rightarrow R)$ ever gets added to the givens list, then we should consider using modus ponens or modus tollens. For now, we need to concentrate on the goal.

The goal is also a conditional statement, so we assume the antecedent and set the consequent as our new goal:

Givens	*Goal*
$P \to (Q \to R)$	$P \to \neg Q$
$\neg R$	

We can also now write a little bit of the proof:

Suppose $\neg R$.
  [Proof of $P \to \neg Q$ goes here.]
Therefore $\neg R \to (P \to \neg Q)$.

We still can't do anything with the givens, but the goal is another conditional, so we use the same strategy again:

Givens	*Goal*
$P \to (Q \to R)$	$\neg Q$
$\neg R$	
P	

Now the proof looks like this:

Suppose $\neg R$.
  Suppose P.
    [Proof of $\neg Q$ goes here.]
  Therefore $P \to \neg Q$.
Therefore $\neg R \to (P \to \neg Q)$.

We've been watching for our chance to use our first given by applying either modus ponens or modus tollens, and now we can do it. Since we know $P \to (Q \to R)$ and P, by modus ponens we can infer $Q \to R$. Any conclusion inferred from the givens can be added to the givens column:

Givens	*Goal*
$P \to (Q \to R)$	$\neg Q$
$\neg R$	
P	
$Q \to R$	

We also add one more line to the proof:

Suppose $\neg R$.
  Suppose P.
    Since P and $P \to (Q \to R)$, it follows that $Q \to R$.
    [Proof of $\neg Q$ goes here.]
  Therefore $P \to \neg Q$.
Therefore $\neg R \to (P \to \neg Q)$.

Finally, our last step is to use modus tollens. We now know $Q \to R$ and $\neg R$, so by modus tollens we can conclude $\neg Q$. This is our goal, so the proof is done.

Solution

Theorem. *Suppose $P \to (Q \to R)$. Then $\neg R \to (P \to \neg Q)$.*
Proof. Suppose $\neg R$. Suppose P. Since P and $P \to (Q \to R)$, it follows that $Q \to R$. But then, since $\neg R$, we can conclude $\neg Q$. Thus, $P \to \neg Q$. Therefore $\neg R \to (P \to \neg Q)$. □

Sometimes if you're stuck you can use rules of inference to work backward. For example, suppose one of your givens has the form $P \to Q$ and your goal is Q. If only you could prove P, you could use modus ponens to reach your goal. This suggests treating P as your goal instead of Q. If you can prove P, then you'll just have to add one more step to the proof to reach your original goal Q.

Example 3.2.5. Suppose that $A \subseteq B$, $a \in A$, and $a \notin B \setminus C$. Prove that $a \in C$.

Scratch work

Givens	*Goal*
$A \subseteq B$	$a \in C$
$a \in A$	
$a \notin B \setminus C$	

Our third given is a negative statement, so we begin by reexpressing it as an equivalent positive statement. According to the definition of the difference of two sets, this given means $\neg(a \in B \land a \notin C)$, and by one of DeMorgan's laws, this is equivalent to $a \notin B \lor a \in C$. Because our goal is $a \in C$, it is probably more useful to rewrite this in the equivalent form $a \in B \to a \in C$:

Givens	*Goal*
$A \subseteq B$	$a \in C$
$a \in A$	
$a \in B \to a \in C$	

Now we can use our strategy for using givens of the form $P \to Q$. Our goal is $a \in C$, and we are given that $a \in B \to a \in C$. If we could prove that $a \in B$, then we could use modus ponens to reach our goal. So let's try treating $a \in B$ as our goal and see if that makes the problem easier:

Givens	*Goal*
$A \subseteq B$	$a \in B$
$a \in A$	
$a \in B \rightarrow a \in C$	

Now it is clear how to reach the goal. Since $a \in A$ and $A \subseteq B$, $a \in B$.

Solution

Theorem. *Suppose that $A \subseteq B$, $a \in A$, and $a \notin B \setminus C$. Then $a \in C$.*

Proof. Since $a \in A$ and $A \subseteq B$, we can conclude that $a \in B$. But $a \notin B \setminus C$, so it follows that $a \in C$. □

Exercises

*1. This problem could be solved by using truth tables, but don't do it that way. Instead, use the methods for writing proofs discussed so far in this chapter. (See Example 3.2.4.)
   (a) Suppose $P \rightarrow Q$ and $Q \rightarrow R$ are both true. Prove that $P \rightarrow R$ is true.
   (b) Suppose $\neg R \rightarrow (P \rightarrow \neg Q)$ is true. Prove that $P \rightarrow (Q \rightarrow R)$ is true.

2. This problem could be solved by using truth tables, but don't do it that way. Instead, use the methods for writing proofs discussed so far in this chapter. (See Example 3.2.4.)
   (a) Suppose $P \rightarrow Q$ and $R \rightarrow \neg Q$ are both true. Prove that $P \rightarrow \neg R$ is true.
   (b) Suppose that P is true. Prove that $Q \rightarrow \neg(Q \rightarrow \neg P)$ is true.

3. Suppose $A \subseteq C$, and B and C are disjoint. Prove that if $x \in A$ then $x \notin B$.

4. Suppose that $A \setminus B$ is disjoint from C and $x \in A$. Prove that if $x \in C$ then $x \in B$.

*5. Use the method of proof by contradiction to prove the theorem in Example 3.2.1.

6. Use the method of proof by contradiction to prove the theorem in Example 3.2.5.

7. Suppose that $y + x = 2y - x$, and x and y are not both zero. Prove that $y \neq 0$.

*8. Suppose that a and b are nonzero real numbers. Prove that if $a < 1/a < b < 1/b$ then $a < -1$.
9. Suppose that x and y are real numbers. Prove that if $x^2y = 2x + y$, then if $y \neq 0$ then $x \neq 0$.
10. Suppose that x and y are real numbers. Prove that if $x \neq 0$, then if $y = \frac{3x^2+2y}{x^2+2}$ then $y = 3$.
*11. Consider the following incorrect theorem:

    Incorrect Theorem. *Suppose x and y are real numbers and $x + y = 10$. Then $x \neq 3$ and $y \neq 8$.*

    (a) What's wrong with the following proof of the theorem?

    Proof. Suppose the conclusion of the theorem is false. Then $x = 3$ and $y = 8$. But then $x + y = 11$, which contradicts the given information that $x + y = 10$. Therefore the conclusion must be true. □

    (b) Show that the theorem is incorrect by finding a counterexample.
12. Consider the following incorrect theorem:

    Incorrect Theorem. *Suppose that $A \subseteq C$, $B \subseteq C$, and $x \in A$. Then $x \in B$.*

    (a) What's wrong with the following proof of the theorem?

    Proof. Suppose that $x \notin B$. Since $x \in A$ and $A \subseteq C$, $x \in C$. Since $x \notin B$ and $B \subseteq C$, $x \notin C$. But now we have proven both $x \in C$ and $x \notin C$, so we have reached a contradiction. Therefore $x \in B$. □

    (b) Show that the theorem is incorrect by finding a counterexample.
13. Use truth tables to show that modus tollens is a valid rule of inference.
*14. Use truth tables to check the correctness of the theorem in Example 3.2.4.
15. Use truth tables to check the correctness of the statements in exercise 1.
16. Use truth tables to check the correctness of the statements in exercise 2.
17. Can the proof in Example 3.2.2 be modified to prove that if $x^2 + y = 13$ and $x \neq 3$ then $y \neq 4$? Explain.

3.3. Proofs Involving Quantifiers

Look again at Example 3.2.3. In that example we said that x could be anything at all, and we proved the statement $x \in A \setminus C \rightarrow x \in B$. Because the reasoning we used would apply no matter what x was, our proof actually shows that $x \in A \setminus C \rightarrow x \in B$ is true for all x. In other words, we can conclude $\forall x(x \in A \setminus C \rightarrow x \in B)$.

This illustrates the easiest and most straightforward way of proving a goal of the form $\forall x P(x)$. If you can give a proof of the goal $P(x)$ that would work no matter what x was, then you can conclude that $\forall x P(x)$ must be true. To make sure that your proof would work for any value of x, it is important to start your proof with no assumptions about x. Mathematicians express this by saying that x must be *arbitrary*. In particular, you must not assume that x is equal to any other object already under discussion in the proof. Thus, if the letter x is already being used in the proof to stand for some particular object, then you cannot use it to stand for an arbitrary object. In this case you must choose a different variable that is not already being used in the proof, say y, and replace the goal $\forall x P(x)$ with the equivalent statement $\forall y P(y)$. Now you can proceed by letting y stand for an arbitrary object and proving $P(y)$.

To prove a goal of the form $\forall x P(x)$:

Let x stand for an arbitrary object and prove $P(x)$. The letter x must be a new variable in the proof. If x is already being used in the proof to stand for something, then you must choose an unused variable, say y, to stand for the arbitrary object, and prove $P(y)$.

Scratch work

Before using strategy:

Givens	*Goal*
—	$\forall x P(x)$
—	

After using strategy:

Givens	*Goal*
—	$P(x)$
—	

Form of final proof:

Let x be arbitrary.
[Proof of $P(x)$ goes here.]
Since x was arbitrary, we can conclude that $\forall x P(x)$.

Example 3.3.1. Suppose A, B, and C are sets, and $A \setminus B \subseteq C$. Prove that $A \setminus C \subseteq B$.

Scratch work

Givens	*Goal*
$A \setminus B \subseteq C$	$A \setminus C \subseteq B$

As usual, we look first at the logical form of the goal to plan our strategy. In this case we must write out the definition of $\subseteq$ to determine the logical form of the goal.

Givens	*Goal*
$A \setminus B \subseteq C$	$\forall x(x \in A \setminus C \to x \in B)$

Because the goal has the form $\forall x P(x)$, where $P(x)$ is the statement $x \in A \setminus C \to x \in B$, we will introduce a new variable x into the proof to stand for an arbitrary object and then try to prove $x \in A \setminus C \to x \in B$. Note that x *is* a new variable in the proof. It appeared in the logical form of the goal as a bound variable, but remember that bound variables don't stand for anything in particular. We have not yet used x as a free variable in any statement, so it has not been used to stand for any particular object. To make sure x is arbitrary we must be careful not to add any assumptions about x to the givens column. However, we do change our goal:

Givens	*Goal*
$A \setminus B \subseteq C$	$x \in A \setminus C \to x \in B$

According to our strategy, the final proof should look like this:

> Let x be arbitrary.
> [Proof of $x \in A \setminus C \to x \in B$ goes here.]
> Since x was arbitrary, we can conclude that $\forall x(x \in A \setminus C \to x \in B)$, so $A \setminus C \subseteq B$.

The problem is now exactly the same as in Example 3.2.3, so the rest of the solution is the same as well. In other words, we can simply insert the proof we wrote in Example 3.2.3 between the first and last sentences of the proof written here.

Solution

Theorem. *Suppose A, B, and C are sets, and $A \setminus B \subseteq C$. Then $A \setminus C \subseteq B$.*

Proof. Let x be arbitrary. Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$. Then $x \in A \setminus B$, so since $A \setminus B \subseteq C, x \in C$. But this contradicts the fact that $x \notin C$. Therefore $x \in B$. Thus, if $x \in A \setminus C$ then $x \in B$. Since x was arbitrary, we can conclude that $\forall x(x \in A \setminus C \rightarrow x \in B)$, so $A \setminus C \subseteq B$. □

Notice that, although this proof shows that every element of $A \setminus C$ is also an element of B, it does not contain phrases such as "every element of $A \setminus C$" or "all elements of $A \setminus C$." For most of the proof we simply reason about x, which is treated as a single, fixed element of $A \setminus C$. We pretend that x stands for some particular element of $A \setminus C$, being careful to make no assumptions about *which* element it stands for. It is only at the end of the proof that we observe that, because x was arbitrary, our conclusions about x would be true no matter what x was. This is the main advantage of using this strategy to prove a goal of the form $\forall x P(x)$. It enables you to prove a goal about *all* objects by reasoning about only *one* object, as long as that object is arbitrary. If you are proving a goal of the form $\forall x P(x)$ and you find yourself saying a lot about "all x's" or "every x," you are probably making your proof unnecessarily complicated by not using this strategy.

As we saw in Chapter 2, statements of the form $\forall x(P(x) \rightarrow Q(x))$ are quite common in mathematics. It might be worthwhile, therefore, to consider how the strategies we've discussed can be combined to prove a goal of this form. Because the goal starts with $\forall x$, the first step is to let x be arbitrary and try to prove $P(x) \rightarrow Q(x)$. To prove this goal, you will probably want to assume that $P(x)$ is true and prove $Q(x)$. Thus, the proof will probably start like this: "Let x be arbitrary. Suppose $P(x)$." It will then proceed with the steps needed to reach the goal $Q(x)$. Often in this type of proof the statement that x is arbitrary is left out, and the proof simply starts with "Suppose $P(x)$." When a new variable x is introduced into a proof in this way, it is usually understood that x is arbitrary. In other words, no assumptions are being made about x other than the stated one that $P(x)$ is true.

An important example of this type of proof is a proof in which the goal has the form $\forall x \in A\ P(x)$. Recall that $\forall x \in A\ P(x)$ means the same thing as $\forall x(x \in A \rightarrow P(x))$, so according to our strategy the proof should start with "Suppose $x \in A$" and then proceed with the steps needed to conclude that $P(x)$ is true. Once again, it is understood that no assumptions are being made about x other than the stated assumption that $x \in A$, so x stands for an arbitrary element of A.

Mathematicians sometimes skip other steps in proofs, if knowledgeable readers could be expected to fill them in themselves. In particular, many of our proof strategies have suggested that the proof end with a sentence that sums up why the reasoning that has been given in the proof leads to the desired conclusion.

In a proof in which several of these strategies have been combined, there might be several of these summing up sentences, one after another, at the end of the proof. Mathematicians often condense this summing up into one sentence, or even skip it entirely. When you are reading a proof written by someone else, you may find it helpful to fill in these skipped steps.

Example 3.3.2. Suppose A and B are sets. Prove that if $A \cap B = A$ then $A \subseteq B$.

Scratch work

Our goal is $A \cap B = A \rightarrow A \subseteq B$. Because the goal is a conditional statement, we add the antecedent to the givens list and make the consequent the goal. We will also write out the definition of $\subseteq$ in the new goal to show what its logical form is.

Givens	*Goal*
$A \cap B = A$	$\forall x(x \in A \rightarrow x \in B)$

Now the goal has the form $\forall x(P(x) \rightarrow Q(x))$, where $P(x)$ is the statement $x \in A$ and $Q(x)$ is the statement $x \in B$. We therefore let x be arbitrary, assume $x \in A$, and prove $x \in B$:

Givens	*Goal*
$A \cap B = A$	$x \in B$
$x \in A$	

Combining the proof strategies we have used, we see that the final proof will have this form:

Suppose $A \cap B = A$.
  Let x be arbitrary.
    Suppose $x \in A$.
      [Proof of $x \in B$ goes here.]
    Therefore $x \in A \rightarrow x \in B$.
  Since x was arbitrary, we can conclude that $\forall x(x \in A \rightarrow x \in B)$, so $A \subseteq B$.
Therefore, if $A \cap B = A$ then $A \subseteq B$.

As discussed earlier, when we write up the final proof we can skip the sentence "Let x be arbitrary," and we can also skip some or all of the last three sentences.

We have now reached the point at which we can analyze the logical form of the goal no further. Fortunately, when we look at the givens, we discover that the goal follows easily. Since $x \in A$ and $A \cap B = A$, it follows that $x \in A \cap B$, so $x \in B$. (In this last step we are using the definition of $\cap$: $x \in A \cap B$ means $x \in A$ and $x \in B$.)

Solution

Theorem. *Suppose A and B are sets. If $A \cap B = A$ then $A \subseteq B$.*

Proof. Suppose $A \cap B = A$, and suppose $x \in A$. Then since $A \cap B = A$, $x \in A \cap B$, so $x \in B$. Since x was an arbitrary element of A, we can conclude that $A \subseteq B$. □

Proving a goal of the form $\exists x P(x)$ also involves introducing a new variable x into the proof and proving $P(x)$, but in this case x will not be arbitrary. Because you only need to prove that $P(x)$ is true for *at least one* x, it suffices to assign a particular value to x and prove $P(x)$ for this one value of x.

To prove a goal of the form $\exists x P(x)$:

Try to find a value of x for which you think $P(x)$ will be true. Then start your proof with "Let $x =$ (the value you decided on)" and proceed to prove $P(x)$ for this value of x. Once again, x should be a new variable. If the letter x is already being used in the proof for some other purpose, then you should choose an unused variable, say y, and rewrite the goal in the equivalent form $\exists y P(y)$. Now proceed as before by starting your proof with "Let $y =$ (the value you decided on)" and prove $P(y)$.

Scratch work

Before using strategy:

Givens	*Goal*
—	$\exists x P(x)$
—	

After using strategy:

Givens	*Goal*
—	$P(x)$
—	

$x =$ (the value you decided on)

Form of final proof:

Let $x =$ (the value you decided on).
[Proof of $P(x)$ goes here.]
Thus, $\exists x P(x)$.

Finding the right value to use for x may be difficult in some cases. One method that is sometimes helpful is to assume that $P(x)$ is true and then see if you can figure out what x must be, based on this assumption. If $P(x)$ is an equation involving x, this amounts to solving the equation for x. However, if this doesn't work, you may use any other method you please to try to find a value to use for x, including trial-and-error and guessing. The reason you have such freedom with this step is that *the reasoning you use to find a value for x will not appear in the final proof.* This is because of our rule that a proof should only contain the reasoning needed to justify the conclusion of the proof, not an explanation of how you thought of that reasoning. To justify the conclusion that $\exists x P(x)$ is true it is only necessary to verify that $P(x)$ comes out true when x is assigned some particular value. How you thought of that value is your own business, and not part of the justification of the conclusion.

Example 3.3.3. Prove that for every real number x, if $x > 0$ then there is a real number y such that $y(y+1) = x$.

Scratch work

In symbols, our goal is $\forall x(x > 0 \rightarrow \exists y[y(y+1) = x])$, where the variables x and y in this statement are understood to range over $\mathbb{R}$. We therefore start by letting x be an arbitrary real number, and we then assume that $x > 0$ and try to prove that $\exists y[y(y+1) = x]$. Thus, we now have the following given and goal:

Givens	*Goal*
$x > 0$	$\exists y[y(y+1) = x]$

Because our goal has the form $\exists y P(y)$, where $P(y)$ is the statement $y(y+1) = x$, according to our strategy we should try to find a value of y for which $P(y)$ is true. In this case we can do it by solving the equation $y(y+1) = x$ for y. It's a quadratic equation and can be solved using the quadratic formula:

$$y(y+1) = x \quad \Rightarrow \quad y^2 + y - x = 0 \quad \Rightarrow \quad y = \frac{-1 \pm \sqrt{1+4x}}{2}.$$

Note that $\sqrt{1+4x}$ is defined, since we have $x > 0$ as a given. We have actually found two solutions for y, but to prove that $\exists y[y(y+1) = x]$ we only need to exhibit one value of y that makes the equation $y(y+1) = x$ true. Either of the two solutions could be used in the proof. We will use the solution $y = (-1 + \sqrt{1+4x})/2$.

The steps we've used to solve for y should not appear in the final proof. In the final proof we will simply say "Let $y = (-1 + \sqrt{1+4x})/2$" and then prove that $y(y+1) = x$. In other words, the final proof will have this form:

> Let x be an arbitrary real number.
>   Suppose $x > 0$.
>   Let $y = (-1 + \sqrt{1+4x})/2$.
>   [Proof of $y(y+1) = x$ goes here.]
>   Thus, $\exists y[y(y+1) = x]$.
>   Therefore $x > 0 \to \exists y[y(y+1) = x]$.
> Since x was arbitrary, we can conclude that $\forall x(x > 0 \to \exists y[y(y+1) = x])$.

To see what must be done to fill in the remaining gap in the proof, we add $y = (-1 + \sqrt{1+4x})/2$ to the givens list and make $y(y+1) = x$ the goal:

Givens	*Goal*
$x > 0$	$y(y+1) = x$
$y = \dfrac{-1+\sqrt{1+4x}}{2}$	

We can now prove that the equation $y(y+1) = x$ is true by simply substituting $(-1 + \sqrt{1+4x})/2$ for y and verifying that the resulting equation is true.

Solution

Theorem. *For every real number x, if $x > 0$ then there is a real number y such that $y(y+1) = x$.*

Proof. Let x be an arbitrary real number, and suppose $x > 0$. Let

$$y = \frac{-1+\sqrt{1+4x}}{2}$$

which is defined since $x > 0$. Then,

$$\begin{aligned} y(y+1) &= \left(\frac{-1+\sqrt{1+4x}}{2}\right)\cdot\left(\frac{-1+\sqrt{1+4x}}{2}+1\right) \\ &= \left(\frac{\sqrt{1+4x}-1}{2}\right)\cdot\left(\frac{\sqrt{1+4x}+1}{2}\right) \\ &= \frac{1+4x-1}{4} = \frac{4x}{4} = x. \end{aligned}$$

□

Sometimes when you're proving a goal of the form $\exists y Q(y)$ you won't be able to tell just by looking at the statement $Q(y)$ what value you should plug in for y. In this case you may want to look more closely at the givens to see if they suggest a value to use for y. In particular, a given of the form $\exists x P(x)$ may be helpful in this situation. This given says that an object with a certain property exists. It is probably a good idea to imagine that a particular object with this property has been chosen and to introduce a new variable, say x_0, into the proof to stand for this object. Thus, for the rest of the proof you will be using x_0 to stand for some particular object, and you can assume that with x_0 standing for this object, $P(x_0)$ is true. In other words, you can add $P(x_0)$ to your givens list. This object x_0, or something related to it, might turn out to be the right thing to plug in for y to make $Q(y)$ come out true.

To use a given of the form $\exists x P(x)$:

Introduce a new variable x_0 into the proof to stand for an object for which $P(x_0)$ is true. This means that you can now assume that $P(x_0)$ is true. Logicians call this rule of inference *existential instantiation.*

Note that using a given of the form $\exists x P(x)$ is very different from proving a goal of the form $\exists x P(x)$, because when using a given of the form $\exists x P(x)$, *you don't get to choose a particular value to plug in for x.* You can assume that x_0 stands for some object for which $P(x_0)$ is true, but you can't assume anything else about x_0. On the other hand, a given of the form $\forall x P(x)$ says that $P(x)$ would be true *no matter what* value is assigned to x. You can therefore *choose any value you wish* to plug in for x and use this given to conclude that $P(x)$ is true.

To use a given of the form $\forall x P(x)$:

You can plug in any value, say a, for x and use this given to conclude that $P(a)$ is true. This rule is called *universal instantiation.*

Usually, if you have a given of the form $\exists x P(x)$, you should apply existential instantiation to it immediately. On the other hand, you won't be able to apply universal instantiation to a given of the form $\forall x P(x)$ unless you have a particular value a to plug in for x, so you might want to wait until a likely choice for a pops up in the proof. For example, consider a given of the form $\forall x(P(x) \rightarrow Q(x))$. You can use this given to conclude that $P(a) \rightarrow Q(a)$ for any a, but according to our rule for using givens that are conditional statements, this conclusion probably won't be very useful unless you know either $P(a)$ or $\neg Q(a)$. You should probably wait until an object a appears in the proof for which you know either $P(a)$ or $\neg Q(a)$, and plug this a in for x when it appears.

We've already used this technique in some of our earlier proofs when dealing with givens of the form $A \subseteq B$. For instance, in Example 3.2.5 we used the givens $A \subseteq B$ and $a \in A$ to conclude that $a \in B$. The justification for this reasoning is that $A \subseteq B$ means $\forall x(x \in A \rightarrow x \in B)$, so by universal instantiation we can plug in a for x and conclude that $a \in A \rightarrow a \in B$. Since we also know $a \in A$, it follows by modus ponens that $a \in B$.

Example 3.3.4. Suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets and $\mathcal{F} \cap \mathcal{G} \neq \varnothing$. Prove that $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.

Scratch work

Our first step in analyzing the logical form of the goal is to write out the meaning of the subset symbol, which gives us the statement $\forall x(x \in \cap\mathcal{F} \rightarrow x \in \cup\mathcal{G})$. We could go further with this analysis by writing out the definitions of union and intersection, but the part of the analysis that we have already done will be enough to allow us to decide how to get started on the proof. The definitions of union and intersection will be needed later in the proof, but we will wait until they are needed before filling them in. When analyzing the logical forms of givens and goals in order to figure out a proof, it is usually best to do only as much of the analysis as is needed to determine the next step of the proof. Going further with the logical analysis usually just introduces unnecessary complication, without providing any benefit.

Because the goal means $\forall x(x \in \cap\mathcal{F} \rightarrow x \in \cup\mathcal{G})$, we let x be arbitrary, assume $x \in \cap\mathcal{F}$, and try to prove $x \in \cup\mathcal{G}$.

Givens	*Goal*
$\mathcal{F} \cap \mathcal{G} \neq \varnothing$	$x \in \cup\mathcal{G}$
$x \in \cap\mathcal{F}$	

The new goal means $\exists A \in \mathcal{G}(x \in A)$, so to prove it we should try to find a value that will "work" for A. Just looking at the goal doesn't make it clear how to choose A, so we look more closely at the givens. We begin by writing them out in logical symbols:

Givens	*Goal*
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$	$\exists A \in \mathcal{G}(x \in A)$
$\forall A \in \mathcal{F}(x \in A)$	

The second given starts with $\forall A$, so we may not be able to use this given until a likely value to plug in for A pops up during the course of the proof. In