7
Styles of Proof

EARLIER, WE PRACTICED PROVING the validity of logical arguments, both with and without quantifiers. The technique introduced there is one of the main tools for constructing proofs in a more general setting. In this chapter, various common styles of proof in mathematics are described. Recognizing these styles of proof will make both reading and constructing proofs a little less onerous.

The example proofs in this chapter will use some familiar facts about integers, which we will prove in a later chapter.

7.1 Direct proof

As mentioned before, the typical form of the statement of a theorem is: *if a and b and c and* $\cdots$*, then d*. The propositions a,b,c, $\cdots$ are called the hypotheses, and the proposition d is called the conclusion. The goal of the proof is to show that $(a \wedge b \wedge c \wedge \cdots) \rightarrow d$ is a true proposition. In the case of propositional logic, the only thing that matters is the *form* of a logical argument, not the particular propositions that are involved. That means the proof can always be given in the form of a truth table. In areas outside of propositional logic that is no longer possible. Now the content of the propositions must be considered. In other words, what the words mean, and not merely how they are strung together, becomes important.

Suppose we want to prove an implication **Theorem:** *If p, then q*. In other words, we want to show $p \rightarrow q$ is true. There are two possibilities: Either p is false, in which case $p \rightarrow q$ is automatically true, or p is true. In this second case, we need to show that q is true as well to conclude $p \to q$ is true. In other words, to show $p \to q$ is true, we can begin by assuming p is true, and then give an *argument* that q must be true as well. The outline of such a proof will look like:

Proof:

Step 1)	Reason 1
Step 2)	Reason 2
$\vdots$	$\vdots$
Step l)	Reason l

♣

Every step in the proof must be a true proposition, and since the goal is to conclude q is true, the proposition q will be the last step in the proof. **There are only four acceptable reasons** that can be invoked to justify a step in a proof. Each step can be: (1) a *hypothesis* (and so assumed to be true), (2) an application of a *definition*, (3) a *known fact* proved previously, and so known to be true, or (4) a consequence of applying a *rule of inference or a logical equivalence* to earlier steps in the proof. The only difference between these sorts of formal proofs and the proofs of logical arguments we practiced earlier is the inclusion of definitions as a justification of a step.

Before giving a few examples, there is one more point to consider. Most theorems in mathematics involve variables in some way, along with either universal or existential quantifiers. But, in the case of universal quantifiers, tradition dictates that the mention of the quantifier is often suppressed, and left for the reader to fill in. For example consider: **Theorem:** *If n is an even integer, then n^2 is an even integer*. The statement is really shorthand for **Theorem:** *For every $n \in \mathbb{Z}$, if n is even, then n^2 is even*. If we let $E(n)$ be the predicate *n is even* with universe of discourse $\mathbb{Z}$, the theorem becomes **Theorem:** $\forall n(E(n) \to E(n^2))$. The truth of such a universally quantified statement can be accomplished with an application of the rule of universal generalization. In other words, we prove that for an arbitrary $n \in \mathbb{Z}$, the proposition $E(n) \to E(n^2)$ is true. The result is stated and proved in the next theorem.

Theorem 7.1. *If n is an even integer, then n^2 is an even integer.*

Proof.

1) n is an even integer	hypothesis
2) $n = 2k$ for an integer k	definition of even
3) $n^2 = 4k^2$	algebra fact
4) $n^2 = 2(2k^2)$	algebra fact
5) n^2 is even	definition of even

♣

Usually proofs are not presented in the dry stepwise style of the last example. Instead, a more narrative style is used. So the above proof could go as follows:

Proof. *Suppose n is an even integer. That means $n = 2k$ for some integer k. Squaring both sides gives $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ which shows n^2 is even.* ♣

All the ingredients of the stepwise proof are present in the narrative form, but this second form is a little more reader friendly. For example, we can include a few comments, such as *squaring both sides gives* to help the reader figure out what is happening.

The method of proof given above is called **direct proof**. The characteristic feature of a direct proof is that in the course of the proof, the hypotheses appear as steps, and the last step in the proof is the conclusion of the theorem.

It is traditional to put a marker (such as ♣, to indicate the theorem has been **clubbed**!) at the end of a narrative form of a proof to let the reader know the proof is complete.

Here is one more example of a direct proof.

Theorem 7.2. *If n and m are odd integers, then $n + m$ is even.*

Proof. *Suppose m and n are odd integers. That means $m = 2j + 1$ for some integer j, and $n = 2k + 1$ for some integer k. Adding gives $m + n = (2j + 1) + (2k + 1) = 2j + 2k + 2 = 2(j + k + 1)$, and so we see $m + n$ is even.* ♣

7.2 *Indirect proof*

There are cases where a direct proof is not very convenient for one reason or another. There are several other styles of proof, each based on some logical equivalence.

For example, since $p \to q \equiv \neg q \to \neg p$, we can prove the

Theorem 7.3. $p \to q$

by instead giving a proof of

Theorem 7.4. $\neg q \to \neg p.$

In other words, we replace the requested implication with its contrapositive, and prove that instead. This method of proof is called **indirect proof**. Here's an example.

Theorem 7.5. *If m^2 is an even integer, then m is an even integer.*

Proof. *Suppose m is not even. Then m is odd. So $m = 2k + 1$ for some integer k. Squaring both sides of that equation gives $m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which shows m^2 is not even.* ♣

Notice that we gave a *direct proof* of the equivalent theorem: *If m is not an even integer, then m^2 is not an even integer*.

7.3 *Proof by contradiction*

Another alternative to a direct proof is **proof by contradiction**. In this method the plan is to replace the requested **Theorem:** r (where r can be any simple or compound proposition) with **Theorem:** $\neg r \to \mathbb{F}$, where $\mathbb{F}$ is any proposition known to be false. The reason proof by contradiction is a valid form of proof is that $\neg r \to \mathbb{F} \equiv r$, so that showing $\neg r \to \mathbb{F}$ is true is identical to showing r is true. Proofs by contradiction can be a bit more difficult to discover than direct or indirect proofs. The reason is that in those two types of proof, we know exactly what the last line of our proof will be. We know where we want to get to. But in a proof by contradiction, we only know that we want to end up with some (any) proposition known to be false. Typically, when writing a proof by contradiction, we experiment, trying various logical arguments, hoping to stumble across some false proposition, and so conclude the proof. For example, consider the following.

Theorem 7.6. *$\sqrt{2}$ is irrational.*

The plan is to replace the requested theorem with

Theorem 7.7. *If $\sqrt{2}$ is rational, then $\mathbb{F}$ (some fact known to be false).*

And now, we may give a direct proof of this replacement theorem:

Proof. *Suppose that $\sqrt{2}$ is rational. Then there exist integers m and n with $n \neq 0$, so that $\sqrt{2} = \frac{m}{n}$, with $\frac{m}{n}$ in lowest terms. Squaring both sides gives $2 = \frac{m^2}{n^2}$. Thus $m^2 = 2n^2$ and so m^2 is even. Therefore m is even. So $m = 2k$ for some integer k. Substituting $2k$ for m in $m^2 = 2n^2$ shows $(2k)^2 = 4k^2 = 2n^2$. Which means that $n^2 = 2k^2$. Therefore n^2 is even, which means n is even. Now since both m and n are even, they have 2 as a common factor. Therefore $\frac{m}{n}$ is in lowest terms and it is not in lowest terms. $\rightarrow\!\leftarrow$.* ♣

The symbol $\rightarrow\!\leftarrow$ (two arrows crashing into each other head on) denotes that we have reached a *fallacy* ($\mathbb{F}$), a statement known to be false. It usually marks the end of a proof by contradiction.

In the next example, we will prove a proposition of the form $p \to q$ by contradiction. The theorem is about real numbers x and y.

Theorem 7.8. *If $0 < x < y$, then $\sqrt{x} < \sqrt{y}$.*

Think of the statement of the theorem in the form $p \to q$. The plan is to replace the requested theorem with

Theorem 7.9. $\neg(p \to q) \to \mathbb{F}$.

But $\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$. So we will actually prove $(p \wedge \neg q) \to \mathbb{F}$. In other words, we will prove (directly)

Theorem 7.10. *If $0 < x < y$ and $\sqrt{x} \geq \sqrt{y}$, then (some fallacy).*

Proof. *Suppose $0 < x < y$ and $\sqrt{x} \geq \sqrt{y}$. Since $\sqrt{x} > 0$, $\sqrt{x}\sqrt{x} \geq \sqrt{x}\sqrt{y}$, which is the same as $x \geq \sqrt{xy}$. Also, since $\sqrt{y} > 0$, $\sqrt{y}\sqrt{x} \geq \sqrt{y}\sqrt{y}$, which is the same as $\sqrt{xy} \geq y$. Putting $x \geq \sqrt{xy}$ and $\sqrt{xy} \geq y$ together, we conclude $x \geq y$. Thus $x < y$ and $x \geq y$. $\rightarrow\!\leftarrow$* ♣

7.4 *Proof by cases*

The only other common style of proof is **proof by cases**. Let's first look at the justification for this proof technique. Suppose we are asked to prove

Theorem 7.11 (Theorem X)**.** *$p \to q$.*

We *dream up* some propositions, r and s, and replace the requested theorem with three theorems:

Theorem 7.12 (Theorem XS)**.** *(1) $p \longrightarrow (r \vee s)$, (2) $r \to q$, and (3) $s \to q$.*

The propositions r, s we dream up are called the *cases*. There can be any number of cases. If we dream up three cases, then we would have four theorems to prove, and so on. The hope is that the proofs of these replacement theorems will be much easier than a proof of the original theorem. [1]

The reason proof by cases is a valid proof technique is that

$$[(p \longrightarrow (r \vee s)) \wedge (r \to q) \wedge (s \to q)] \to (p \to q)$$

is a tautology[2]. Proof by cases, as for proof by contradiction, is generally a little trickier than direct and indirect proofs. In a proof by contradiction, we are not sure exactly what we are shooting for. We just hope some contradiction will pop up. For a proof by cases, we have to dream up the cases to use, and it can be difficult at times to dream up good cases.

Theorem 7.13. *For any integer n, $|n| \geq n$.*

Proof. *Suppose n is an integer. There are two cases:Either (1): $n > 0$, or (2): $n \leq 0$.*

This has the form $p \longrightarrow (r \vee s)$ of (1) in Theorem 7.4.

Case 1: We need to show If $n > 0$, then $|n| \geq n$. (We will do this with a direct proof.) Suppose $n > 0$. Then $|n| = n$. Thus $|n| \geq n$ is true.

Case 2: We need to show If $n \leq 0$, then $|n| \geq n$. (We will again use a direct proof.) Suppose $n \leq 0$. Now $0 \leq |n|$. Thus, $n \leq |n|$.

So, in any case, $n \leq |n|$ is true, and that proves the theorem. ♣

[1] This is the *divide and conquer* approach to a proof.

[2] Prove this!

7.5 Existence proof

A proof of a statement of the form $\exists x P(x)$ is called an **existence proof**. The proof may be **constructive**, meaning that the proof provides a specific example of, or at least an explicit recipe for finding, an x so that $P(x)$ is true; or the proof may be **non-constructive**, meaning that it establishes the existence of x without giving a method of actually producing an example of an x for which $P(x)$ is true.

To give examples of each type of existence proof, let's use a familiar fact (which will be proved a little later in the course): There are infinitely many primes. Recall that a prime is an integer greater than 1 whose only positive divisors are 1 and itself. The next two theorems are contrived, but they demonstrate the ideas of constructive and nonconstructive proofs.

Theorem 7.14. *There is a prime with more than two digits.*

Proof. *Checking shows that* 101 *has no positive divisors besides* 1 *and itself. Also,* 101 *has more than two digits. So we have produced an example of a prime with more than two digits.* ♣

That is a constructive proof of the theorem. Now, here is a nonconstructive proof of a similar theorem.

Theorem 7.15. *There is a prime with more than one billion digits.*

Proof. *Since there are infinitely many primes, they cannot all have one billion or fewer digits. So there must some primes with more than one billion digits.* ♣

7.6 Using a counterexample to disprove a statement

Finally, suppose we are asked to prove a theorem of the form $\forall x\ P(x)$, and for one reason or another we come to believe the proposition is not true. The proposition can be shown to be false by exhibiting a specific element from the domain of x for which $P(x)$ is false. Such an example is called a **counterexample** to the theorem. Let's look at a specific instance of the counterexample technique.

Theorem 7.16 (not really!). *For all positive integers* n, $n^2 - n + 41$ *is prime*

Counterexample. *To disprove the theorem, we explicitly specify a positive integer* n *such that* $n^2 - n + 41$ *is not prime. In fact, when* $n = 41$*, the expression is not a prime since clearly* $41^2 - 41 + 41 = 41^2$ *is divisible by* 41*. So,* $n = 41$ *is a counterexample to the proposition.* ♣

An interesting fact about this example is that $n = 41$ is the smallest counterexample. For $n = 1, 2, \cdots 40$, it turns out that $n^2 - n + 41$ is a prime! This examples shows the danger of checking a theorem of the form $\forall x\, P(x)$ for a few (or a few billion!) values of x, finding $P(x)$ true for those cases, and concluding it is true for every possible value of x.

For the purpose of these exercises and problems, feel free to use familiar facts and definitions about integers. For example: Recall, an integer n is even if $n = 2k$ for some integer k. And, an integer n is odd if $n = 2k + 1$ for some integer k.

7.7 *Exercises*

Exercise 7.1. *Give a direct proof that the sum of two even integers is even.*

Exercise 7.2. *Give an indirect proof that if the square of the integer n is odd, then n is odd.*

Exercise 7.3. *Give a proof by contradiction that the sum of a rational number and an irrational number is irrational.*

Exercise 7.4. *Give a proof by contradiction that if* $5n - 1$ *is odd, then n is even.*

Exercise 7.5. *In Chapter 1, exercise f), you concluded that If* $x = 2$, *then* $x^2 - 2x + 1 = 0$ *is not a proposition. Using the convention given in this chapter, what would you say now, and why?*

Exercise 7.6. *Give a counterexample to the proposition Every positive integer that ends with a* 7 *is a prime.*

7.8 Problems

Problem 7.1. *Give a direct proof that the sum of an even integer and an odd integer is odd.*

Hint: Start by letting m be an even integer and letting n be an odd integer. That means $m = 2k$ for some integer k and $n = 2j + 1$ for some integer j. You are interested in $m + n$, so add them up and see what you get. Why is the thing you get an odd integer (think about the definition of odd)?

Problem 7.2. *Give a direct proof that the sum of two odd integers is even.*

Problem 7.3. *Give an indirect proof that if n^3 is even, then n is even. Hint: Study the solution of a similar statement in the sample exercises for this lesson.*

Problem 7.4. *Give a proof by contradiction that if $3n + 2$ is odd, then n is odd.*

Hint: This is the problem in this set that gives the most grief. Study the section in the notes where the mechanics of proving a statement of the form If P, then Q by contradiction is discussed. Be sure you understand why the first line of the proof should be something like Suppose $3n + 2$ is odd **and** *n is even.*

Problem 7.5. *Give an example of a predicate $P(n)$ about positive integers n, such that $P(n)$ is true for every positive integer from 1 to one billion, but which is never-the-less not true for all positive integers. (Hint: there is a really simple choice possible for the predicate $P(n)$.)*

Problem 7.6. *The* ***maximum*** *of two numbers, a and b is a provided $a \geq b$. Notation: $\max(a, b) = a$. The* ***minimum*** *of a and b is a provided $a \leq b$. Notation: $\min(a, b) = a$. Examples: $\max(2, 3) = 3$, $\max(5, 0) = 5$, $\min(2, 3) = 2$, $\min(5, 0) = 0$, $\max(4, 4) = \min(4, 4) = 4$.*

Give a proof by cases that for any numbers s, t,

$$\min(s, t) + \max(s, t) = s + t.$$

Problem 7.7. *Give a proof by cases that for integers m, n, we have $|mn| = |m||n|$. Hint: Consider four cases: (1) $m \geq 0$ and $n \geq 0$, (2) $m \geq 0$ and $n < 0$, (3) $m < 0$ and $n \geq 0$, and (4) $m < 0$ and $n < 0$.*