Chapter 5

Indirect ("Contra") Proofs

With direct proofs covered (see the previous chapter), we can consider two proof techniques that are variations of direct proof: Proof by Contraposition (a slight variation) and Proof by Contradiction (a not-as-slight variation). These are sometimes known as 'indirect' proof techniques because they are, well, not direct.[1]

5.1 Proof by Contraposition

Sometimes, a conjecture's hypothesis doesn't provide much useful information with which to start a direct proof. We've seen that, with a little creativity, we can sometimes extract enough information to make a direct proof possible (e.g., Example 84 in Chapter 4). When you are faced with a conjecture whose conclusion seems to be a better source of information than does the hypothesis, a *proof by contraposition* might be a better choice of proof technique. *proof by contraposition*

The name "proof by contraposition" completely reveals the difference between it and a direct proof: Instead of proving the given conjecture as-is, we prove its contrapositive. This technique is still logically valid because, as we learned in Chapter 1, an implication and its contrapositive are equivalent: $p \to q \equiv \neg q \to \neg p$. And so, in a proof by contraposition:

$$\boxed{\text{To prove } p \to q\text{: Assume } \neg q\text{, show } \neg p.}$$

Other than that, everything about a proof by contraposition is the same as for a direct proof. To make the reader's life a little easier, start such

[1] Proof techniques just don't have superhero-esque origin stories.

proofs with "Proof (by Contraposition):" or "Proof (Contrapositive):", but otherwise, you already know what do to (and what not to do!).

indirect proof

Proof by contraposition is sometimes referred to as a form of *indirect proof*, although that term is most frequently applied to proof by contradiction (see Section 5.2). The term fits here because we aren't simply assuming p and showing q. Proofs by contradiction are even less direct, which is probably why most people reserve the term to describe that technique.

Because proofs by contraposition are very similar to direct proofs, we will give just two examples, enough to highlight the utility of the technique.

Example 92:

Problem: Prove that if $a - b$ is an irrational number, then a is irrational or b is irrational, where $a, b \in \mathbb{R}$.

Solution: To use a direct proof here, we need to know something useful about irrational numbers as a starting point for the argument. We know that any real number that isn't expressible as a ratio of integers is irrational, but that doesn't seem like much of a starting point for a direct proof. However, it can be useful in a proof by contraposition, because using contraposition means introducing negations, and a real number that is not irrational is rational – and something we can easily represent.

In a proof by contraposition, we will need to assume the negation of the original conclusion and show the negation of the original hypothesis. Let's start with the original conclusion: "a is irrational or b is irrational". The disjunction appears to be inclusive (there are no linguistic clues to the contrary). By one of De Morgan's laws, its negation is "a is rational and b is rational". We can work with that. Our new conclusion, the negation of the original hypothesis, is "$a-b$ is rational". That also seems manageable.

Actually, it's more than just manageable; it's quite straight-forward, as is the entire proof: We will represent a and b as ratios of integers and use basic algebra to demonstrate that their difference is also a ratio of integers.

Proof (Contraposition): We are assuming that a and b are both rational numbers. We need to show that their difference $(a-b)$ is also a rational number.

Rational numbers can be expressed as ratios of integers. Let $a = \frac{c}{d}$ and $b = \frac{e}{f}$, where $c, d, e, f \in \mathbb{Z}$. $a - b = \frac{c}{d} - \frac{e}{f} = \frac{cf}{df} - \frac{de}{df} = \frac{cf-de}{df}$, which is a ratio of integers. Thus, $a-b$ is a rational number.

Therefore, if $a-b$ is an irrational number, then a is irrational or b is irrational, where $a, b \in \mathbb{R}$.

The value of stating the assumed information is greater in contrapositive proofs than in direct proofs, because, having had to rewrite the hypotheses and conclusions, mistaking the old for the new is a potential problem. Writing out the contrapositive's hypothesis and conclusion can help prevent that problem from occurring. We won't usually state the new assumption and conclusion as plainly as we did here, but we do recommend the practice.

Please notice that we concluded the proof by restating the original conjecture, not its contrapositive equivalent. The reason for this is that we were asked to show the truth of the original conjecture. It is appropriate to end by stating that we have shown what we were asked to show.

The next example shows a problem that can occur if one is too eager to attempt a direct proof, and how trying a different proof technique can avoid the problem.

Example 93:

Problem: Prove that if $y^2 + y \leq xy + x$, then $y \leq x,\ x, y \in \mathbb{R}$.

Solution: If your mind is open to contrapositives, you'll look at this conjecture and see that it fits that form very nicely. If you're still locked into direct proofs, you might look at the hypothesis and notice that $y+1$ can be factored from both sides, leading to this straight-forward but in-valid argument:

'Proof' (Direct):

$$\begin{array}{rcll} y^2+y & \leq & xy+x & \text{[Given]} \\ y(y+1) & \leq & x(y+1) & \text{[Factoring]} \\ y & \leq & x & \text{[Divide both sides by } (y+1)\text{]} \end{array}$$

Therefore, $y \leq x$.

Do you see the error in the reasoning? If not, spend a few minutes thinking about it before moving onto the next paragraph.

There are actually two problems, one more immediate than the other. The immediate problem is with the division. x and y, we were told, can be any real numbers. -1 is a real number, and when $y = -1$, moving from the second line to the third is a division by zero.

The less-immediate problem got overlooked in our rush to choose a proof technique: Multiplying (or dividing) both sides of an inequality by a negative number changes its direction. This conjecture is not true for nearly all negative reals.

Time to fix these problems. So that we have something provable, let's change the domain to the positive reals (that is, $x, y \in \mathbb{R}^+$).[2] The new domain eliminates the division by zero concern, meaning that we could use the direct proof. We'll do it with contraposition anyway, so that you can compare the techniques.

Proof (Contraposition): Assume that $y > x$. We need to show that $y^2 + y > xy + x$.

$$\begin{array}{rcll} y & > & x & \text{[Given]} \\ y(y+1) & > & x(y+1) & \text{[Multiply both sides by } (y+1)\text{]} \\ y^2+y & > & xy+x & \text{[Multiply through]} \end{array}$$

Therefore, if $y^2 + y \leq xy + x$, then $y \leq x,\ x, y \in \mathbb{R}^+$.

Using a proof by contraposition allows us to start with a simple hypothesis and build toward the conclusion. This 'simple-to-complex' progression is often the most straight-forward way to develop an argument.

Final note: Are you thinking that we should be assuming $y \geq x$ instead of $y > x$? If so, you're forgetting that the negation of $\leq$ is $>$.

5.1.1 Disproofs and Contraposition

Just as there's no special connection between direct proofs and disproofs, there's also nothing special about disproving conjectures that initially appeared to be good candidates for proof by contraposition. The techniques presented in the previous chapter (Chapter 4) are still the ones to use.

5.2 Proof by Contradiction

In Chapter 3 we presented example dialog that mentioned 'reductive' reasoning. We deferred discussion of it to this chapter because well-structured reductive reasoning is also known as *proof by contradiction*. The idea is easy to state but harder to explain: We assume that the conclusion is false and reason until we reach a logical contradiction. *proof by contradiction*

At first read, that statement might seem like a big pile of shhhh. . .aving cream,[3] but it is entirely logical. Here's how it turns out to be a valid argument.

Proof by contraposition works because the contrapositive of the conjecture is logically equivalent to the conjecture. It's tempting to look through our tables of logical equivalences from Chapter 1 to see if there are any others that look promising. The Law of Implication seems simple enough, but it turns an implication into an inclusive-OR. There are three ways for an inclusive-OR to be true (that's three cases to have to prove), plus we lose the conclusion. Simple, but not very helpful.

[2]Does it feel like we're cheating by changing the problem? If this were a homework or exam, of course we wouldn't change it; rather, we'd ask if there's a typo or if a disproof is acceptable. We're trying to make a point about thinking before doing, and to demonstrate proof by contradiction. Having learned about disproofs in the last chapter, you should be able to disprove this conjecture with its original domain. Give it a try!

[3]Be nice and clean! Shave every day and you'll always look keen! (Apologies to Benny Bell, author of the 1946 song "Shaving Cream.")

Another promising equivalence is $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow \mathbf{F}$, known as *reductio ad absurdum*. There's no inclusive-OR to worry about, and we still have a conclusion ... but it's just 'false.' How can we reason toward 'false?' We learned two ways in Chapter 1: Use a truth table that shows all inputs evaluating to 'false,' or create a logical equivalence argument that ends at 'false.' Either way, we demonstrate a contradiction.[4] In a more free-form proof, like those of this chapter, we can accomplish the same thing by reasoning until we discover a result (say, $\overline{x}$) that is the opposite of something we already know (x). Both $\overline{x}$ and x cannot be true. Assuming that we started with the correct compound hypotheses ($p \wedge \neg q$), and that our reasoning was logical, arriving at a contradiction (that is, arriving at $\mathbf{F}$) means that the original conjecture must be true, by *reductio ad absurdum*.

Here's another way to look at how a proof by contradiction works. Start with a basic conjecture: $p \rightarrow q$. We believe it to be true, otherwise we wouldn't be trying to prove it. That means we believe $\neg(p \rightarrow q)$ to be false. Because $\neg(p \rightarrow q) \equiv \neg(\neg p \vee q) \equiv \neg\neg p \wedge \neg q \equiv p \wedge \neg q$, we must also believe $p \wedge \neg q$ to be false. If we reason starting from $p \wedge \neg q$ and encounter a contradiction, as long as our reasoning was good, the only part of the argument that could have been false was the assumption, and therefore its opposite – the given conjecture $p \rightarrow q$ – must be true.

Still not really buying it? We understand; this isn't easy for most people to follow the first time, or the second, or maybe even the nineteenth. Keep thinking about it; if you followed the logic behind proof by contraposition, you can get your mind around proof by contradiction, too. At a minimum, we're confident that you understand why proof by contradiction is also known as indirect proof!

In the meantime, take a look at that assumption again: $p \wedge \neg q$. To be allowed to assume both p and $\neg q$, imagine that we made a deal with the Deity of Arguments.[5] The Deity of Arguments was sympathetic to our need for more given information, and was willing to help, but, needing to save face with the other deities, required something in return: We had to sacrifice the conclusion in exchange for more given information. Having accepted this deal with the deity, our fate is to reason blindly until we stumble upon some sort of contradiction – we have no idea when or where it will appear.[6]

[4] Contradiction ... proof by contradiction ... coincidence? Yeah, right.

[5] Yes, a relative of the Deity of Partial Credit; naturally, they're both from the same pantheon: The one from which no big-budget action movie will ever be made.

[6] For the sake of your grade on a future quiz or exam, if asked to explain the logical justification for a proof by contradiction, don't answer "The Deity of Arguments gave it to us!" We gave you two lovely, serious explanations; answer using one of those instead.

For many people, proof by contradiction's lack of a clear target makes applying it a significant challenge. Other people really take to it, to the point that proof by contradiction is their first choice whenever a proof is needed. If you find that proof by contradiction really 'sings' to you, try to remember to use it only when it makes sense to do so.

That's a key question: When does it make sense to use a proof by contradiction? Direct proofs are useful when p gives enough information. Proofs by contraposition are useful when $\neg q$ gives enough. If neither p nor $\neg q$ give enough by themselves, perhaps their combination $(p \wedge \neg q)$ does. That's when a proof by contradiction may be the best choice.

In summary:

$$\boxed{\text{To prove } p \rightarrow q\text{: Assume } p \wedge \neg q\text{, show a contradiction.}}$$

To show how and when to use a proof by contradiction, we have three examples. The first one is pretty simple . . . maybe *too* simple.

Example 94:

Problem: Prove that if $a \,\%\, 3 = 1$ and $b \,\%\, 3 = 2$, then $3 \mid (a + b)$.

Solution: First things first: We need to remind ourselves what the notation is trying to tell us. $a \,\%\, 3 = 1$ means that a is one more than a multiple of three. Similarly, $b \,\%\, 3 = 2$ means b is two more (or one less) than a multiple of three. $3 \mid (a+b)$ means that $a+b$ is exactly a multiple of three.

To prove this by contradiction, we assume $a \,\%\, 3 = 1$, $b \,\%\, 3 = 2$, and $3 \nmid (a + b)$ (the negation of $3 \mid (a + b)$). $3 \nmid (a + b)$ means that $a + b$ isn't a multiple of three; that is, $(a + b) \,\%\, 3$ is either one or two.

If you're thinking, "Wait; 'either one or two?' Doing this by contradiction seems to be making this harder, not easier!", you're forgiven. As usual, we chose this example to demonstrate the proof technique and to make a point.

Proof (Contradiction): Assume that $a \,\%\, 3 = 1$, $b \,\%\, 3 = 2$, and $3 \nmid (a+b)$. Because a is one more than a multiple of three, we can represent a with $3k+1$, where $k \in \mathbb{Z}$. Similarly, we will represent b with $3j+2$, where $j \in \mathbb{Z}$.

$a + b = (3k + 1) + (3j + 2) = 3k + 3j + 3 = 3(k + j + 1)$. This shows that $a+b$ is a multiple of three; that is, $3 \mid (a+b)$. However, we assumed that $3 \nmid (a+b)$. No value can both be and not be a multiple of three; this is a contradiction.

Therefore, if $a \,\%\, 3 = 1$ and $b \,\%\, 3 = 2$, then $3 \mid (a+b)$.

Although our discussion ahead of the proof made it seem that things were going to get messy ("$(a+b) \,\%\, 3$ is either one or two"), we didn't need to reach that level of detail in the proof. Sometimes, the preparation is worse than the proof.

Speaking of messes, here's the point we want to make about proving the conjecture of Example 94 using contradiction: We really don't need an indirect proof to do it; a direct proof will work just fine. (For practice, create one!) Some snooty proof experts will tell you that it's not appropriate to use contradiction when the resulting contradiction is with one of the givens. Unfortunately, it can be hard to see that that will occur before you write the proof. We aren't that snooty; we're happy to accept the contradiction whenever and wherever we find it.

Example 95:

Problem: One of our example conjectures in Chapter 4 ("if gh is odd, then g and h are both odd" from Example 84) required us to consider three cases when we did it with a direct proof. Would doing it with a proof by contradiction be easier?

Solution: This is the sort of question that's good to ask yourself when you're working on a homework assignment (but not-so-good to ponder during an exam!). You've completed a proof, and you could turn it in

...but that annoying voice in the back corner of your brain is telling you that you can do better. Let's humor that voice and see if we can do better with a proof by contradiction.

Using contradiction, we get to assume that "gh is odd" is true, and also that the negation of "g and h are both odd" is true. But what is that negation? It's tempting just to flip 'odd' to 'even,' but that's not the correct negation. "g and h are both odd" is a short-cut way of saying "g is odd and h is odd." To negate that, we need to haul out one of De Morgan's Laws. The resulting negation is "g is even or h is even." Thus, we can assume g is even and h is odd, or g is odd and h is even, or that both g and h are even. As with Example 94, this is starting to sound like a lot of work. Maybe it will be, maybe it won't; there's one sure way to find out: Try it!

Proof (Contradiction): Assume that gh is odd, and that g is even or h is even (or both). If only one variable is even, it doesn't matter which one, because we are going to create the product gh and multiplication is commutative. If both are even, we can again assume that either one is even. WLOG, let g be even and equal to $2k$, $k \in \mathbb{Z}$. $gh = (2k)h = 2(kh)$, by associativity of multiplication. This shows that gh must be even, a contradiction of our assumption that gh is odd.

Therefore, if gh is odd, then g and h are both odd.

This is much shorter than the direct proof we created for this conjecture. It's so short that, by comparison, you might be worried that something's wrong with it. There isn't; the brevity can be attributed to the use of a more appropriate proof technique.

Actually, it could be quite a bit shorter. In many textbooks, authors would skip the justification ahead of the 'WLOG,' leaving that for the readers to puzzle out on their own. In a class in which you are learning to write proofs, be safe and include the justification. Now, if we wanted to make the proof longer,[7] we could have considered all three cases separately, much as we did in the direct proof. Thanks to our knowledge of multiplication, there was no need to do that.

Example 95 shows how choosing the appropriate proof technique can save time. Even so, it isn’t a ‘classic’ proof by contradiction, because it contradicted a piece of assumed information. The next example is even better, because the conjecture would be very difficult to prove with another technique.

Example 96:

Problem: Prove that $\log_3 4$ is irrational.

Solution: This is another conjecture not in ‘if – then’ form. There’s a good reason for that: There isn’t a specific hypothesis, just the desired conclusion. For such conjectures, a proof by contradiction is often a good choice, because it allows us to use (the negation of) the only available piece of information as our starting point.

We know that a real number that is not irrational is rational. We will represent $\log_3 4$ with a fraction, and use our knowledge of logarithms to take us to a contradiction.

[7] Why?!? For the love of the Deity of Arguments, why?

Proof (Contradiction): Assume that $\log_3 4$ is rational. Let $\log_3 4 = \frac{n}{d}$, where $n, d \in \mathbb{Z}^+$. By the relationship between logarithms and exponents, we can rewrite this as $3^{n/d} = 4$. Raising both sides to the power of d gives $(3^{n/d})^d = 4^d$, which means $3^{(n/d)\cdot d} = 4^d$, or $3^n = 4^d$.

Observe that $\log_3 4$ is more than one (because $\log_3 3 = 1$ and log is an increasing function) and less than two ($\log_3 9 = 2$). This means that $n > d > 1$, and thus $n - 1$ and $d - 1$ are integers that are ≥ 1.

$3^n = 3^{n-1} \cdot 3$, which is an odd times an odd. We learned, in Example 77 of Chapter 4, that the product of two odds is odd. $4^d = 4^{d-1} \cdot 4$, which is an even times an even. The project of two evens must be even ($(2k)(2j) = 2(2kj)$). Because 3^n is odd and 4^d is even, $3^n \neq 4^d$. This contradicts the earlier observation that $3^n = 4^d$.

Therefore, $\log_3 4$ is irrational.

We have several things to say about the proof of Example 96.

- This proof is a good example of how 'classic' contradiction proofs work: We reasoned for a while and discovered something ($3^n = 4^d$). Then, we reasoned some more on a different fact and discovered a contradictory piece of information ($3^n \neq 4^d$). Neither of those were given to us; we had to uncover them ourselves.

- You probably noticed that we snuck[8] in a mini-lemma to show that the product of two evens is even. It would be more proper to have a separate lemma to show this, but as we're now quite familiar with manipulating evens and odds, we decided to use a short-cut.

[8]'Sneaked' is considered to be better for formal writing than is 'snuck.' Since when has this book been an exemplar of formal writing?

If you're wondering why we didn't just reference the lemma from Example 80 in Chapter 4, note that it specifically covers only the case of an even number times itself, not the case of an even times a potentially different even. They are closely related, but are not the same. It would be appropriate to say that the evenness of an even times itself is a corollary of the evenness of an even times an even, but our examples weren't set up in that order.

- The proof's little digression into the characteristics of $n-1$ and $d-1$ is the sort of discussion that most proofs would assume the reader could figure out on their own. We decided to include it because (a) when exponents are negative, we leave the realm of integers (and therefore of evens and odds), and (b) showing that $d-1 \geq 1$ meant that we didn't have to worry about $4^0 \cdot 4$ (an odd times an even).

- Tired of evens and odds? Want a different way to reach a contradiction? We could have used this approach for the last half of the proof: The only factors of 3^n are powers of 3, and the only factors of 4^d are powers of 4. Because n and d are greater than zero, there's no way for 3^n to equal 4^d.

- Are you wondering if we could have used a proof by contraposition instead? Yes, we could have, but we would have created a proof by contradiction wearing a proof by contraposition costume. Here's what we mean: As we know, in a proof by contraposition of $p \to q$, we assume $\neg q$ and show $\neg p$. We weren't given a hypothesis, which means $p \equiv \mathbf{T}$ (we could have written the conjecture as "if true, then $\log_3 4$ is irrational"). In a proof by contraposition, then, we'd get to assume that $\log_3 4$ is rational (just like the proof by contradiction) and would need to show false (again, just like the proof by contradiction). Might as well just do a proof by contradiction!

5.3 Proving Biconditional Conjectures

Most of our conjectures have been (or could be) expressed as "for all" implications. So far we've ignored another kind of "for all" conjecture that can also be expressed as implications: Biconditionals. Happily, proving a biconditional does not require another proof technique. Unhappily, proving a biconditional requires that we construct two proofs.

We hope you remember that a biconditional is defined in terms of implication and AND: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$. This equivalence tells us what we must do to prove a biconditional:

$$\boxed{\text{To prove } p \leftrightarrow q\text{: Prove both } p \rightarrow q \text{ and } q \rightarrow p.}$$

Be aware that you may "mix-n-match" proof techniques when proving a biconditional; that is, you may use a different technique for the "if" half than you used for the "only if" half. Of course, using the same technique for both halves is fine.

To construct a proof of a biconditional conjecture, we have two choices:

1. Write separate, stand-alone proofs of $p \rightarrow q$ and $q \rightarrow p$, and refer to them as lemmas in the (very short) proof of $p \leftrightarrow q$.
2. Include the proofs of $p \rightarrow q$ and $q \rightarrow p$ as cases within the proof of $p \leftrightarrow q$.

We have two examples of biconditional proofs, one for each option.

Example 97:

Problem: Prove that s and t are odd iff st is odd.

Solution: We have already done most of the work for this proof. Example 77 proved "if x and y are odd, then xy is odd," and Example 84 proved the "if gh is odd, the g and h are odd." All we need to do is reference those results as lemmas within our proof of the biconditional.

Proof (Direct): In Example 77, we proved the "only if" half (s and t are odd only if st is odd). In Example 84, we proved the "if" half (s and t are odd if st is odd). Together, these lemmas complete the proof of the biconditional.

Therefore, s and t are odd iff st is odd.

Of course, much of the time we need to prove both halves. The next example shows how to handle this situation.

Example 98:

Problem: Prove that $a^2 + 2a + b^2 - 6b + 10 = 0$ iff $a = -1$ and $b = 3$.

Solution: The "if" half of this is easily proven – we just plug in the given values for a and b and verify that the result is zero.

The "only if" direction requires more imagination. It's tempting to do a little re-arranging ($a^2 + 2a + b^2 - 6b + 10 = a(a+2) + b(b-6) + 10$), but that doesn't seem helpful (how will that tell us what a and b must be?). Instead, we might look at $a^2 + 2a$ and $b^2 - 6b$ and think about completing the squares by finding a way to divide up the 10 between them. This occurs to us because the form $x^2 + yx + z$ is familiar to us, and because specific values for a and b remind us of roots of quadratics. The source of $a^2 + 2a$ could be $(a+1)^2$: $(a+1)^2 = a^2 + 2a + 1$. That leaves 9 for $b^2 - 6b$, and happily $b^2 - 6b + 9 = (b-3)^2$.

We've learned that $a^2 + 2a + b^2 - 6b + 10 = (a+1)^2 + (b-3)^2$. Now we need a convincing argument that the only way for $(a+1)^2 + (b-3)^2$ to equal zero is for a to be -1 and for b to be 3. We know that the square of any real will be non-negative, which means that the only way to get a sum of zero is $0 + 0$. The only way for $(a+1)^2$ to equal zero is for a to be -1, and the only way for $(b-3)^2$ to equal zero is for b to be 3. We've got our argument.

Proof (Cases): To prove the biconditional we need to prove the two component conjectures individually.

Case 1: We use a direct proof to show that $a^2+2a+b^2-6b+10=0$ if $a=-1$ and $b=3$.

> Replacing a and b with the given values, we find that $(-1)^2+2(-1)+(3)^2-6(3)+10 = 1-2+9-18+10 = 0$. Thus, $a^2+2a+b^2-6b+10=0$ if $a=-1$ and $b=3$.

Case 2: We use a direct proof to show that $a^2+2a+b^2-6b+10=0$ only if $a=-1$ and $b=3$.

> $a^2+2a+b^2-6b+10 = a^2+2a+1+b^2-6b+9 = (a+1)^2+(b-3)^2$. As x^2 is ≥ 0 for any real number x, the only way for $(a+1)^2+(b-3)^2$ to equal 0 is for $(a+1)^2=0$ and $(b-3)^2=0$. The roots of these quadratics are -1 and 3, respectively, establishing that $a=-1$ and $b=3$. Thus, $a^2+2a+b^2-6b+10=0$ only if $a=-1$ and $b=3$.

Therefore, $a^2+2a+b^2-6b+10=0$ iff $a=-1$ and $b=3$.

In a biconditional proof, our preferred "Proof (*technique*)" label can be more awkward than helpful, because we could use one proof technique for the "if" and another for the "only if." As each case is a separate proof, it's reasonable to mention the technique at the start of each case, and to say at the top that we're doing a proof by cases, as we did here. But, as we used direct proofs in both cases, we could have used our usual format instead.

5.4 Summary of Direct and Indirect Proof Techniques

Figure 5.1 summarizes the three major proof techniques covered in the past two chapters.

The algorithm given in Figure 5.2 offers suggestions for choosing a proof technique. This algorithm is not meant to be inflexible; it has value in that in can help novice proof-writers decide how to begin. Remember, false starts

Proof Technique	(Assume) Hypothesis	(Show) Conclusion
Direct	p	q
Contraposition	$\neg q$	$\neg p$
Contradiction	$p \wedge \neg q$	A Contradiction

Figure 5.1: The three major proof techniques, their starting points, and their destinations.

If the conjecture ($p \to q$) appears to be true,

    If p provides useful information,
        Try a direct proof
    Otherwise, if $\neg q$ provides useful information,
        Try a proof by contraposition
    Otherwise,
        Try a proof by contradiction

Otherwise,

    If the conjecture is universally quantified,
        Try disproving it with a counter-example
    Otherwise,
        Try disproving it by proving its negation

Figure 5.2: An initial proof technique selection algorithm.

are common in proof-writing. What appears to be a good starting point for a proof may not be upon closer examination. Also, remember that not all proofs are of conjectures of the $p \to q$ form. For instance, the conjecture might be existential, for which a single confirming example will prove that it is true.

