Over-Use of the Method of Contradiction

This handout presents seven examples of proofs that the book suggests you do by the Method of Contradiction, but that are better done without Contradiction. In this handout, I do the proofs two ways: without Contradiction, and then with Contradiction. In every example, you can see that the proof without contradiction is shorter and clearer.

And yet contradiction proofs are very commonly used to prove statements like the ones proven in these examples. This sort of over-use of Contradiction is very common. Learn to recognize it when you are reading proofs, and learn to avoid it when you are writing proofs!

[Example 1] Prove that for all integers m, $3m + 2$ is not divisible by 3.

Proof without contradiction

(1) Suppose that $m \in \mathbb{Z}$
(2) Let $n = 3m + 2$.
(3) n cannot be writen as $n = 3k$ for an integer k. (By the **Quotient Remainder Theorem** with $d = 3$, applied to n).
(4) Therefore, n is not divisible by 3. (by (3) and the **definition of divisible**)

End of Proof

Proof without contradiction

(1) Suppose that $m \in \mathbb{Z}$
(2) Let $n = 3m + 2$.
(3) Assume that n is divisible by 3. (assumption for proof by contradiction).
(4) Then n can be writen as $n = 3k$ for an integer k. (by (3) and the **definition of divisible**)
(5) Then $(n = 3m + 2 \text{ for some } m \in \mathbb{Z}) \wedge (n = 3k \text{ for some } k \in \mathbb{Z})$ (by (2),(3))
(6) Statement (5) is a contradiction (By the **Quotient Remainder Theorem** with $d = 3$, applied to n). Therefore our assumption in step (3) was wrong: n cannot be divisible by 3.

End of Proof

In Epp 4th Edition Exercise 4.6#4, the author suggests that you prove a similar statement by the Method of Contradiction. But you can see that a direct proof is simpler and clearer. In your Suggested Exercises, you're told to prove the statement without the Method of Contradiction.

[Example 2] Prove that there is no greatest integer.

Proof without contradiction

Let S be the following statement.

Statement S: There is no greatest integer.

This could be written more clearly as

Statement S: It is not true that there is greatest integer.

Written formally, this becomes:

$$\text{Statement } S\text{: } \sim\Big(\exists m \in \mathbb{Z}\big(\forall n \in \mathbb{Z}(m \geq n)\big)\Big).$$

Simplifing this by moving the negation as far to the right as possible, we obtain

$$\text{Statement } S\text{: } \forall m \in \mathbb{Z}\big(\exists n \in \mathbb{Z}(n > m)\big).$$

Rewriting this informally, we obtain

Statement S: For every integer, there exists an integer that is larger.

This version of Statement S is very easy to prove.

(1) Suppose that an $m \in \mathbb{Z}$ is given.
(2) Let $n = m + 1$.
(3) Observe that $n \in \mathbb{Z}$ and $n > m$.

End of Proof

Proof by Contradiction.

(1) Assume that there is a greatest integer. Call it m. (Assumption for Proof by Contradiction)
(2) Let $n = m + 1$.
(3) Observe that $n \in \mathbb{Z}$ and $n > m$.
(4) So m is a greatest integer and m is not a greatest integer.
(5) Statement (4) is a conbtradiction. Therefore, our assumption in step (1) was wrong: That is, there is no greatest integer.

End of Proof

In Epp 4th Edition Theorem 4.6.1, the claim is proven by Contradiction. In Exercises 4.6#5,6,7, the author suggests that you prove similar statements by the Method of Contradiction. But you can see that a direct proof is simpler and clearer. In your Suggested Exercises, you're told to prove the similar statements without the Method of Contradiction.

[Example 3] Prove that the square root of any irrational number is irrational.

Proof by contrapositive

Let S be the following statement:

Statement S: The square root of any irrational number is irrational.

It helps to write this in a more clearly quantified form.

Statement S: For any real number, if the number is irrational, then its square root is irrational.

Written formally, this becomes:

$$\text{Statement } S\text{: } \forall x \in \mathbb{R}\big(\text{If } x \notin \mathbb{Q} \text{ then } \sqrt{x} \notin \mathbb{Q}\big)$$

The contrapositive of S is the following statement.

$$\text{contrapositive of } S\text{: } \forall x \in \mathbb{R}\big(\text{If } \sqrt{x} \in \mathbb{Q} \text{ then } x \in \mathbb{Q}\big)$$

This statement is easy to prove.

(1) Suppose that $x \in \mathbb{R}$ and $\sqrt{x}$ is rational.

(2) Then $\sqrt{x} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ and $q \neq 0$. (by (1) and definition of rational)

(3) Then $\left(\sqrt{x}\right)^2 = \left(\frac{p}{q}\right)^2 = \left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = \frac{p^2}{q^2}$

(4) Observe that p^2 and q^2 are both integers and $q^2 \neq 0$ by the zero product property

(5) So $\left(\sqrt{x}\right)^2$ is rational. That is, x is rational. (by (4) and **definition of rational**)

End of Proof

Proof by Contradiction

(1) Assume that the statement is false. That is, assume that there exists a real number x such that x is irrational and $\sqrt{x}$ is rational. (assumption for proof by contradiction)

(2) Then $\sqrt{x} = \frac{p}{q}$ for $p, q \in \mathbb{Z}$ and $q \neq 0$. (by (1) and definition of rational)

(3) then $\left(\sqrt{x}\right)^2 = \left(\frac{p}{q}\right)^2 = \left(\frac{p}{q}\right)\left(\frac{p}{q}\right) = \frac{p^2}{q^2}$

(4) Observe that p^2 and q^2 are both integers and $q^2 \neq 0$ by the zero product property

(5) So $\left(\sqrt{x}\right)^2$ is rational. That is, x is rational. (by (4) and **definition of rational**)

(6) So x is rational and x is irrational.

(7) Statement (6) is a contradiction. Therefore our assumption in step (1) was wrong. The statement cannot be false. So the statement must be true.

End of Proof.

In Epp 4th Edition Exercise 4.6#10, you are told to prove the statement by Contradiction. In Exercises 4.6#24,25,26, the author suggests that you prove similar statements by Contradiction. But you can see that a proof of the contrapositive is simpler and clearer. In your Suggested Exercises, you're told to prove the similar statements by proving the contrapositive.

[Example 4] Let Statement A be the following:

$$\text{Statement } A\text{: } \forall n \in \mathbb{Z}(\text{If } n^2 \text{ is odd then } n \text{ is odd})$$

Prove Statement A by proving its contrapositive.

The contrapositive of A is the following:

$$\text{contrapositive of } A\text{: } \forall n \in \mathbb{Z}(\text{If } n \text{ is even then } n^2 \text{ is even})$$

(1) Suppose $n \in \mathbb{Z}$ and n is even.
(2) Then $n = 2k$ for some integer k. (by (1) and definition of even)
(3) So $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.
(4) Let $j = 2k^2$. Observe that j is an integer and $n^2 = 2j$.
(5) Conclude that n^2 is even (by (4) and definition of even.)

End of proof

Prove Statement A by contradiction.

(1) Assume that Statement A is false. That is, assume that the negation of A is true.
(assumption for proof by contradiction) The negation of A is the following statement:

$$\text{Negation of } A\text{: } \exists n \in \mathbb{Z}(n^2 \text{ is odd and } n \text{ is even})$$

So we are assuming that there exists an integer n such that n^2 is odd and n is even.
(2) Then $n = 2k$ for some integer k. (by (1) and definition of even)
(3) So $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$.
(4) Let $j = 2k^2$. Observe that j is an integer and $n^2 = 2j$.
(5) Conclude that n^2 is even (by (4) and definition of even.)
(6) n^2 is odd and n^2 is even by (1) and (4).
(7) Statement (6) is a contradiction. Therefore our assumption in step (1) was wrong. Statement A cannot be false. So the Statement A must be true.

End of proof

In Epp 4th Edition Exercise 4.6#25, you are told to prove the statement by Contradiction. In Exercises 4.6#24,25,26, the author suggests that you prove similar statements by Contradiction. But you can see that a proof of the contrapositive is simpler and clearer. In your Suggested Exercises, you're told to prove the similar statements by proving the contrapositive.

[Example 5] Let Statement A be the following:

$\forall a, b, r \in \mathbb{R}$ such that $a, b \in \mathbb{Q}$ and $b \neq 0$(If r is irrational then $a + br$ is irrational.)

Prove Statement A by proving its contrapositive.

The contrapositive of A is the following:

$\forall a, b, r \in \mathbb{R}$ such that $a, b \in \mathbb{Q}$ and $b \neq 0$(If $a + br$ is rational then r is rational.)

(1) Suppose $a, b, r \in \mathbb{R}$ and $a, b \in \mathbb{Q}$ and $b \neq 0$ and $a + br$ is rational.

(2) Then $a = \frac{j}{k}$ and $b = \frac{m}{n}$ and $r = \frac{p}{q}$ for some integers j, k, m, n, p, q. (by (1) and definition of rational). Furthermore, we know that k, n, q are non-zero (because those ratios define real numbers) and we know that $m \neq 0$ (because $b \neq 0$). So we have a new equation

$$\frac{j}{k} + \frac{m}{n} \cdot r = \frac{p}{q} \text{ with } k, m, n, q \neq 0$$

(3) This equation can be solved for r:

$$r = \frac{knp - jnq}{kmq}$$

(The details are just algebra. But the key step is that since $k, m, q \neq 0$, we know that their product $kmq \neq 0$, so we can divide by kmq.) Observe that this equation shows that r can be written as a ratio of integers, with the denominator non-zero.

(4) Conclude that r is rational (by (3) and definition of rational.)

End of proof

Prove Statement A by contradiction.

(1) Assume that Statement A is false. That is, assume that the negation of A is true.

(assumption for proof by contradiction) The negation of A is the following statement:

$\exists a, b, r \in \mathbb{R}$ such that $a, b \in \mathbb{Q}$ and $b \neq 0$(r is irrational and $a + br$ is rational.)

So we are assuming that there exists real numbers a, b, r such that $a, b \in \mathbb{Q}$ and $b \neq 0$ and r is irrational and $a + br$ is rational.

(2) Then $a = \frac{j}{k}$ and $b = \frac{m}{n}$ and $r = \frac{p}{q}$ for some integers j, k, m, n, p, q. And, we know that k, n, q are non-zero and we know that $m \neq 0$ (same justifications as above). So we have an equation

$$\frac{j}{k} + \frac{m}{n} \cdot r = \frac{p}{q} \text{ with } k, m, n, q \neq 0$$

(3) This equation can be solved for r (Same justifications as above.)

$$r = \frac{knp - jnq}{kmq}$$

(4) Conclude that r is rational (by (3) and definition of rational.)

(5) r is irrational and r is rational by (1) and (4).

(6) Statement (5) is a contradiction. Therefore our assumption in step (1) was wrong. Statement A cannot be false. So the Statement A must be true.

End of proof

[Example 6] Let Statement A be the following:

$$\forall a, b, c \in \mathbb{Z}(\text{If } a \nmid bc \text{ then } a \nmid b)$$

Prove Statement A by proving its contrapositive.

The contrapositive of A is the following:

$$\forall a, b, c \in \mathbb{Z}(\text{If } a|b \text{ then } a|bc)$$

(1) Suppose $a, b, c \in \mathbb{Z}$ and $a|b$.
(2) Then $b = aj$ for some integer j (by (1) and definition of divides)
(3) Then $bc = (aj)c = a(jc)$
(4) Let $k = jc$. Then k is an integer and $bc = ak$.
(5) Conclude that $a|bc$ (by (4) and definition of divides.)

End of proof

Prove Statement A by contradiction.

(1) Assume that Statement A is false. That is, assume that the negation of A is true.
(assumption for proof by contradiction) The negation of A is the following statement:

$$\exists a, b, c \in \mathbb{Z}(a \nmid bc \text{ and } a|b)$$

So we are assuming that there exist integers a, b, c such that $a \nmid bc$ and $a|b$.
(2) Then $b = aj$ for some integer j (by (1) and definition of divides)
(3) Then $bc = (aj)c = a(jc)$
(4) Let $k = jc$. Then k is an integer and $bc = ak$.
(5) Conclude that $a|bc$ (by (4) and definition of divides.)
(6) $a \nmid bc$ and $a|bc$ by (1) and (4).
(7) Statement (6) is a contradiction. Therefore our assumption in step (1) was wrong. Statement A cannot be false. So the Statement A must be true.

End of proof

[Example 7] Prove that the set of all prime numbers is an infinite set.

Solution:

It is helpful to rewrite the statement as a universal conditional.

Let Statement A be the following:

$\forall$sets P of prime numbers(If P is the set of all prime numbers then P is not a finite set)

Prove Statement A by proving its contrapositive.

The contrapositive of A is the following:

$\forall$sets P of prime numbers(If P is a finite set then P is not the set of all prime numbers)

(1) Suppose P is a set of prime numbers and that P is a finite set.

(2) Then $P = \{p_1, p_2, \dots, p_k\}$ for some prime numbers $p_1, p_2, \dots, p_k$ (by (1) and definition of finite set.)

(3) Let n be the product of all elements of P. That is, $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$

(4) Observe that every $p_j \in P$ is a divisor of n. That is, $p_j | n$.

(5) Then p_j is *not* a divisor of $n + 1$. That is, $p_j \nmid (n + 1)$. (Here we have used the little theorem that says if a prime p divides n, then p does not divide $n + 1$. That is, if $p|n$ then $p \nmid (n + 1)$.)

(6) The integer $n + 1$ has a prime factorization (by the Unique Factorization Theorem (UFT)) and none of the primes in that factorization can be in set P (by (5)), so there must be a prime that is not in set P. Conclude that P is not the set of all prime numbers.

End of proof

Prove Statement A by contradiction.

(1) Assume that Statement A is false. That is, assume that the negation of A is true. (assumption for proof by contradiction)

The negation of A is the following statement:

The set of all prime numbers is a finite set.

We can denote the set of all prime numbers by the letter P. So are assuming that

The set P of all prime numbers is a finite set.

(2)Then $P = \{p_1, p_2, \dots, p_k\}$ for some prime numbers $p_1, p_2, \dots, p_k$. (by (1) and definition of finite set.)

(3) Let n be the product of all elements of P. That is, $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$

(4) Observe that every $p_j \in P$ is a divisor of n. That is, $p_j | n$.

(5) Then p_j is *not* a divisor of $n + 1$. That is, $p_j \nmid (n + 1)$. (Here we have used the little theorem that says if a prime p divides n, then p does not divide $n + 1$. That is, if $p|n$ then $p \nmid (n + 1)$.)

(6) The integer $n + 1$ has a prime factorization (by the Unique Factorization Theorem (UFT)) and none of the primes in that factorization can be in set P (by (5)), so there must be a prime that is not in set P. Conclude that P is not the set of all prime numbers.

(7) So P is the set of all prime numbers and P is not the set of all prime numbers (1) and (6).

(8) Statement (7) is a contradiction. Therefore our assumption in step (1) was wrong. Statement A cannot be false. So the Statement A must be true.

End of proof