Topic for this Video:

Section 4.7: Indirect Argument: Contradiction and Contraposition

Notice that Section 4.7 is the first section of Chapter 4 that has a title that *does not* start with the words *Direct Proof*.

Section 4.1: Dirct Proof and Counterexample I: Introduction

Section 4.2: Dirct Proof and Counterexample II: Writing Advice

Section 4.3: Direct Proof and Counterexample III: Rational Numbers

Section 4.4: Direct Proof and Counterexample IV: Divisibility

Section 4.5: Direct Proof and Counterexample V:
Division into Cases and the Quotient-Remainder Theorem

Section 4.6: Direct Proof and Counterexample VI: Floor and Ceiling

Section 4.7: Indirect Argument: Contradiction and Contraposition

Section 4.8: Indirect Argument: Two Famous Theorems

From that you should infer two things.

- From the fact that *indirect proofs* are not presented in the book until after six book sections about *direct proofs*, you can infer that *indirect proofs*, whatever they are, are harder or more confusing than *direct proofs*.
- From the fact that there are six book sections about *direct proofs* and only two sections about *indirect proofs*, you can infer that *indirect proofs* are not needed as often as ~~*indirect proofs*~~ *direct*.

I have found that students often use indirect proofs in situations where an indirect proof is not appropriate. The results are always confusing and incorrect proofs.

A colleague has an opinion about why this happens. He thinks that students

- are often confused about the mathematical statements that they are being asked to prove
- are also confused about indirect proofs

As a result, they assume that the proof structure that they don't understand must be the proof structure needed to prove the statement that they don't understand.

It does not help that in math books, *indirect proofs* are often used in places where a *direct proof* would be simpler and clearer. That makes those proofs much harder to read. Even in our book, which is very well written, I find that *indirect proofs* are overused. For instance, I feel that many of the Section 4.7 examples that use indirect proofs, and exercises that ask the student to use indirect proofs, can be more simply done, more clearly done, with direct proofs! That means that the student reading our book might get the wrong idea about how often indirect proofs are actually needed.

In this video, I will focus on two things

- teaching you methods of indirect proof
- pointing out situations where indirect proofs are used or suggested but direct proofs would be better

Both of these things will help make you a better *writer* of proofs. They will also help you become a better, and more critical, *reader* of proofs.

I will begin by doing some examples where the proof methods that we have already learned work just fine. This serves two purposes.

- It gives us a chance to review our proof methods.
- When we revisit these same examples and write indirect proofs, we will see how much more confusing, and how unnecessry, the indirect proof structure is.

Review the method of *Generalizing from a Generic Particular Element*

Recall that the method of *Generalizing from the Generic Particular Element* is used to prove a *universal statement*.

The Method of Generalizing from a Generic Particular Element

To prove statement S of the form

$$\forall x \in D\big(Q(x)\big)$$

Proof (by method of Generalizing from the Generic Particular Element)

(1) Suppose that $x \in D$ (a *generic particular element*)

some steps here

(*) Therefore, $Q(x)$. (with some justification given.)

End of Proof

[Example 1] (4.7#7) Prove that there is no least positive rational number.

Name our statement S

S: It is not true that there exists a least positive rational number.

Rewrite S formally

$$S \equiv \sim(\exists r \in \mathbb{Q}^+ (\forall q \in \mathbb{Q}^+ (r \leq q)))$$

$$\equiv \forall r \in \mathbb{Q}^+ (\sim(\forall q \in \mathbb{Q}^+ (r \leq q)))$$

$$\equiv \forall r \in \mathbb{Q}^+ (\exists q \in \mathbb{Q}^+ (\sim(r \leq q)))$$

$$\equiv \forall r \in \mathbb{Q}^+ (\exists q \in \mathbb{Q}^+ (q < r))$$

Prove S: $\forall r \in \mathbb{Q}^+ \left(\exists q \in \mathbb{Q}^+ (q < r) \right)$

(1) Suppose $r \in \mathbb{Q}^+$ (generic particular element)

(2) There exist positive integers m, n such that $r = \frac{m}{n}$ (by (1) and definition of rational)

(3) Let $q = \frac{m}{2n} = \frac{1}{2} r$

Observe: q is a rational number, because $m, 2n$ are integers and $2n \neq 0$

q is positive, because $m, 2n$ are positive

$q < r$

(4) $\exists q \in \mathbb{Q}^+ (q < r)$ (by 3)

End of Proof

Review Divisibility and the Quotient Remainder Theorem

Recall that the following statement involving the concept of ***divisibility***

$$n \text{ is divisible by } 3$$

means

$$\text{There exists an integer } q \text{ such that } n = 3q$$

And recall the **Quotient Remainder Theorem**

Given any integer n and any positive integer d,

there exist unique integers q and r such that $n = dq + r$ and $0 \leq r < d$

Formal (symbolic)presentation:

$$\forall n \in \boldsymbol{Z}, d \in \boldsymbol{Z}^{+} \left(\exists ! \, q, r \in \boldsymbol{Z} \big((n = dq + r) \wedge (0 \leq r < d) \big) \right)$$

And recall that in the previous video, we discussed the following question.

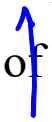
Suppose that n is an integer.

What does the Quotient Remainder Theorem with $d = 3$ tell us about n?

To answer this, we rewrote the *Quotient Remainder Theorem* using $d = 3$ and realized that it amounts to the following OR statement.

$$\big(\exists q \in \boldsymbol{Z}(n = 3q + 0)\big) \vee \big(\exists q \in \boldsymbol{Z}(n = 3q + 1)\big) \vee \big(\exists q \in \boldsymbol{Z}(n = 3q + 2)\big)$$

And in fact, it should really be an EXCLUSIVE OR statement, because exactly one of the three possibilities is true. So the *Quotient Remainder Theorem* with $d = 3$ tells us when writing $n = 3q + r$ in special QRT form (that is, with $0 \leq r < 3$), the remainder r has to be exactly one of the numbers $0,1,2$.



Comparing statement involving the concept of ***divisibility*** and the statement obtained from the ***Quotient Remainder Theorem***, we can see that the statement

n is divisible by 3

means the same thing as this statement

when $n = 3q + r$ is in special QRT form (that is, $0 \leq r < 3$), the remainder $r = 0$.

[Example 2] (Exercise 4.7#4) Prove that for every integer n, $3n + 2$ is not divisible by 3.

Statement written formally

$\forall n \in \mathbb{Z}$ ($3n+2$ is not divisible by 3)

Proof

(1) Suppose $n \in \mathbb{Z}$ (generic particular element)

(2) Let $m = 3n + 2$

Observe that this equation is in QRT form with $d=3$,
because the remainder $r=2$ satisfies $0 \leq 2 < 3$

Since the remainder $r=2$ is not zero,
we conclude that m is not divisible by 3.

(3) $3n+2$ is not divisible by 3

End of Proof

Review the method of *Direct Proof*

When thie method of *Generalizing from a Generic Particular Element* is used to prove a *universal conditional statement*, the resulting structure is called the method of *Direct Proof*.

The Method of Direct Proof

To prove statement S of the form

$$\forall x \in D\big(If\ P(x)\ then\ Q(x)\big)$$

Proof (by method of Direct Proof)

(1) Suppose $x \in D$ and $P(x)$ (a *generic particular element* satisfying the *hypothesis*)

some steps here

(*) Therefore, $Q(x)$. (with some justification given.)

End of Proof

Proving the Contrapositive

Recall that a conditional statement is logically equivalent to its contrapositive.

$$S\text{: } If\ P\ then\ Q$$

is logically equivalent to

$$contrapositive(S)\text{: } If\ {\sim}Q\ then\ {\sim}P$$

The same is true for *universal conditional statements*. That is, they are logically equivalent to their *contrapositives*.

$$S\text{: } \forall x \in D\big(If\ P(x)\ then\ Q(x)\big)$$

is logically equivalent to

$$contrapositive(S)\text{: } \forall x \in D\big(If\ {\sim}Q(x)\ then\ {\sim}P(x)\big)$$

In many situations, it is possible to prove a universal conditional statement S very simply by proving $contrapositive(S)$. Since $contrapositive(S)$ is a universal conditional statement, the proof structure will be *direct proof*.

[Example 3] Prove statement S:

$$\forall n \in \boldsymbol{Z}(If\ n^2\ is\ odd\ then\ n\ is\ odd)$$

The contrapositive(S) is this statement

$\forall n \in \mathbb{Z}$ (If n is even then n^2 is even)

Proof (Direct Proof)

(1) Suppose $n \in \mathbb{Z}$ and n is even. (generic particular element)

(2) There exists an integer k such that $n = 2k$ (by (1) and definition of even)

(3) So $n^2 = (2k)^2$ (by (2))

$= 4k^2 = 2(2k^2)$

(4) Let $j = 2k^2$ Observe that j is an integer and $n^2 = 2j$

(5) There exists an integer j such that $n^2 = 2j$

(6) Therefore n^2 is even (by (5) and definition of even)

End of proof

[Example 4] Prove statement S:

$\forall n \in \mathbb{Z}$

~~$\forall a, b, c \in \mathbb{Z}$~~$(If\ 5 \nmid n^2\ then\ 5 \nmid n)$

Write the contrapositive of S

$\forall n \in \mathbb{Z}$ (If $5 | n$ then $5 | n^2$)

Proof

(1) Suppose $n \in \mathbb{Z}$ and $5 | n$ (generic particular element)

(2) There exists an integer k such that $n = 5k$ (by (1) and definition of Divides)

(3) Then $n^2 = (5k)^2$ (by (2))

$= 25k^2 = 5 \cdot (5k^2)$

(4) Let $j = 5k^2$ Observe that k is an integer and $n^2 = 5j$

(5) There exists an integer j such that $n^2 = 5j$

(6) Therefore $5 | n^2$ (by (5) and definition of Divides)

End of proof.

Review *Contradiction* and *Contradictory Statements*

We say that the statement form

$$(x = 5) \wedge (x = 7)$$

is a ***contradiction***, because when any value of x is substituted in to create an actual statement, the resulting statement will be ***false***.

When x represents a particular (but unnamed) real number, the expression

$$(x = 5) \wedge (x = 7)$$

Represents a ***false statement***. We say that this *statement* is a *contradiction* because the *corresponding statement form* is a contradiction.

If, in a list of statements, we find

some statements

(13) the statement $(x = 5)$

some more statements

(17) the statement $(x = 7)$

We say that statements (13) and (17) are ***contradictory statements***.

Of course, any time a list of statements contains two contradictory statements, they can be used to form a contradiction:

some statements

(13) the statement $(x = 5)$

some more statements

(17) the statement $(x = 7)$

(18) the statement $(x = 5) \wedge (x = 7)$ (by statements (13) and (17))

We say that statements (13) and (17) are ***contradictory statements***.

We say that statement (18) is a ***contradiction***.

Because it is always possible to form a contradiction once two contradictory statements have been written, it is customary say that a contradiction has been reached, even if the contradiction has not been written down as its own statement.

some statements

(13) the statement $(x = 5)$

some more statements

(17) the statement $(x = 7)$

(18) We have reached a contradiction (statement (17) contradicts (13))

In other words, officially to say

We have reached a contradiction.

should mean

We have reached a statement that is a contradiction.

But in practice, it is common to say

We have reached a contradiction.

to mean

We have reached a statement that contradicts some earlier statement.

We say that statements (13) and (17) are ***contradictory statements***.

We say that statement (18) is a ***contradiction***.

Proof by *Contradiction*

Recall again the *Rules of Inference* (which are just known *Valid Argument Forms*).

TABLE 2.3.1 Valid Argument Forms

Modus Ponens	$p \to q$ p $\therefore q$	**Elimination**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalization	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Proof by Division into Cases**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Specialization	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	**Contradiction Rule**	$\sim p \to \mathbf{c}$ $\therefore p$

$\sim P \to C$

$\therefore P$

the letter c denotes a contradiction

A statement form that is always false.

Or a statement that has the form of a contradiction.

Use a truth table to verify that the Contradiction Rule is really a valid argument form

P	~P	C	~P → C
T	F	F	T
F	T	F	F

hypothesis

critical row

Contradiction Rule

~P → C

∴ P

In every critical row, the conclusion is true.

So the argument form is valid.

The *Contradiction Rule* can be used for a proof structure, called the *Method of Contradiction*.

The Method of Contradiction

To prove statement P

Proof (by Method of Contradiction)

(1) Assume P is false. That is, assume $\sim P$ is true. Write out $\sim P$ clearly. (assumption for proof by contradiction)

some steps here

(*) Some contradiction is reached. (Or some statement is written that contradicts an earlier statement). (Explain clearly what the contradiction is.)

(**) So our assumption in step (1) must be wrong. P can't be false. Therefore P is true.

End of Proof

[Example 5] (4.7#18) Prove the following:

If a and b are rational numbers, $b \neq 0$, and x is irrational, then $a + bx$ is irrational.

Write this statement formally

$P \equiv \forall a \in \mathbb{Q}, b \in \mathbb{Q}^*, x \text{ irrational } (a+bx \text{ is irrational})$

$\sim P \equiv \sim(\forall a \in \mathbb{Q}, b \in \mathbb{Q}^*, x \text{ irrational } (a+bx \text{ is irrational}))$

$\equiv \exists a \in \mathbb{Q}, b \in \mathbb{Q}^*, x \text{ irrational } (\sim (a+bx \text{ is irrational}))$

$\equiv \exists a \in \mathbb{Q}, b \in \mathbb{Q}^*, x \text{ irrational } (a+bx \text{ is rational})$

Proof (proof by contradiction)

(1) Assume P is false, that is assume $\sim P$.

$$\exists a \in \mathbb{Q}, b \in \mathbb{Q}^*, x \text{ irrational} \quad (\ a+bx \text{ is rational}\ )$$

(2) There exist integers j, k, with $k \neq 0$, such that $a = \frac{j}{k}$ (by (1) and definition of rational)

(3) There exist integers m, n with $m \neq 0, n \neq 0$ such that $b = \frac{m}{n}$ (by (1) and definition of $\mathbb{Q}^*$)

(4) There exist integers p, q, with $q \neq 0$, such that $a+bx = \frac{p}{q}$ (by (1) and definition of rational)

(5) So $a+bx = \left(\frac{j}{k}\right) + \left(\frac{m}{n}\right)x = \frac{p}{q}$ (substituted 2,3 into 4)

(6) Solve this equation for x

$$\left(\frac{m}{n}\right)x = \frac{p}{q} - \frac{j}{k} = \frac{pk - jq}{qk}$$

↑ get common denominator

(7) multiply both sides by $\frac{n}{m}$

$$x = \frac{n}{m}\left(\frac{pk - jq}{qk}\right) = \frac{n(pk-jq)}{qkm}$$

(8) Observe that $n(pk-jq)$ is an integer

and qkm is a non-zero integer (because q, k, m are all non-zero)

Therefore x is rational.

(9) Observe that statement (8) contradicts statement III.

Conclude that our assumption in Step (1) was wrong.

P cannot be false.

P must be true.

End of Proof

Examples where Proof by Contradiction Method is Unnecessary

Revisit **[Example 1]** (4.7#7) Prove that there is no least positive rational number.

Solution

Statement P there is no least positive rational number

Statement $\sim P$ there is a least positive rational number

$\exists p \in \mathbb{Q}^+ (\forall q \in \mathbb{Q}^+ (p \leq q))$

Proof of P (method of contradiction)

(1) Assume P is false. That is, assume $\sim P$ is true

That is, assume that there is a smallest positive rational number

Call it r.

So r is the smallest positive rational number.

(2) Then there exist positive integers m, n such that $r = \frac{m}{n}$

(by (1) and definition of positive rational number)

(3) Let $q = \frac{m}{2n}$

notice that m, $2n$ are positive integers (by (2))

(4) So q is a positive rational number (by (3) and definition of $\mathbb{Q}^+$)

(5) Also notice that $q = \left(\frac{1}{2}\right)\frac{m}{n}$, so $q < r$.

So r is not the smallest positive rational number.

(6) Observe that (5) contradicts (1). So our assumption in (1) was wrong.

That is, P cannot be false. Conclude that P is true.

End of proof.

Revisit **[Example 2]** (Exercise 4.7#4)

Prove that for every integer n, $3n + 2$ is not divisible by 3.

Statement P: $3n+2$ is not divisible by 3

Statement $\sim P$: $3n+2$ is divisible by 3

Proof of P (by contradiction)

(1) Assume P is false. That is, assume $\sim P$ is true.
So $3n+2$ is divisible by 3

(2) There exists an integer k such that $3n+2=3k$
(by (1) and definition of divisible)

(3) $k = \frac{3n+2}{3} = \frac{3n}{3} + \frac{2}{3} = n + \frac{2}{3}$

So k is not an integer.

(4) Observe that (3) contradicts (2). So our assumption in (1) was wrong. P cannot be false.
Therefore P must be true.

End of proof

Proving the Contrapositive versus Proving by Contradiction

Revisit **[Example 3]** Prove statement S:

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

$\sim S \equiv \sim(\forall n \in \mathbb{Z}$ (If n^2 is odd then n is odd)

$\equiv \exists n \in \mathbb{Z}$ ($\sim$(If n^2 is odd then n is odd)

$\equiv \exists n \in \mathbb{Z}$ ((n^2 is odd) and $\sim$(n is odd))

$\equiv \exists n \in \mathbb{Z}$ ((n^2 is odd) and (n is even))

Proof of S (using method of contradiction)

(1) Assume that S is false. That is, assume ~S is true.

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

(2) Let n be an integer such that n^2 is odd and n is even.
(such an integer is guaranteed to exist by 1)

(3) So n is an even integer (by 2)

(4) There exists an integer k such that $n = 2k$ (by (3) and definition of even)

(5) So $n^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2)$
(by (4))

(6) Let $j = 2k^2$. Observe that j is an integer and $n^2 = 2j$

(7) Therefore n^2 is even (by (6) and definition of even)

(8) Observe that (7) contradicts (2). So our assumption in step (1) must be wrong. S cannot be false

Therefore S is True.

End of Proof.

Notice that this proof by contradiction is 8 statements and, like all contradiction proofs, is a little confusing.

But notice that steps (3)-(7) amount to a proof that

If n is even then n^2 is even,

This is the contrapositive of S.

So the proof of that statement is completely adequate as a proof of S.
(thats what we did in [Example 3])

Putting these steps (3)-(7) inside the frame of a proof by contradiction makes the resulting proof more difficult and less clear.

Wrap Up

Proof by the Method of Contradiction is confusing, both for the writer and the reader. For that reason, it is always best to avoid it if possible.

In many situations, a *universal statement*

$$\forall x \in D\big(Q(x)\big)$$

or a *universal conditional statement*

$$\forall x \in D\big(If\ P(x)\ \ then\ \ Q(x)\big)$$

can be proven using the method of *Generalizing from the Generic Particular* or the method of *Direct Proof*. In those situations, it is definitely best to avoid proof by contradiction.

(that's what we did in [Example 1] and [Example 2])

And in many situations, a *universal conditional statement*

$$\forall x \in D\big(If\ P(x)\ then\ Q(x)\big)$$

can be proven using the method of *Direct Proof* to prove the *contrapositive* statement.

$$\forall x \in D\big(If\ {\sim}Q(x)\ \ then\ \ {\sim}P(x)\big)$$

That is, one supposes that ${\sim}Q(x)$ is true and somehow shows that ${\sim}P(x)$ is true.

We did this in [Example 3] and [Example 4]

(Our book calls this sort of proof an *indirect proof*, but I think that's silly. It is simply a *Direct Proof* of the *contrapositive*. The *contrapositive* is logically equivalent to the *original* statement, so proving the *contrapositive* is equivalent to proving the *original*.)

But there are definitely instances where a *proof by contradiction* is the best method. Proofs by contradiction are by their nature confusing to write and confusing to read. Therefore, it is important to make the proof structure as clear as possible.

We did a proof by contradiction in [Example 5]