8. Proof Strategies

Proof Strategies:

- ☐ Direct proof of $P \to Q$
- ☐ Indirect proof of $P \to Q$

PROOF BY CASES

To prove a statement, such as $P \to Q$, using a PROOF BY CASES, we will

- Break P up into cases $P_1, P_2, \ldots, P_n$ such that $P \equiv P_1 \vee P_2 \vee \cdots \vee P_n$.
- Then, prove each of the conditional statements

$$\begin{aligned} P_1 &\to Q \\ P_2 &\to Q \\ &\vdots \\ P_n &\to Q \end{aligned}$$

  using whichever strategy seems best.
- Because the cases $P_1, P_2, \ldots, P_n$ capture all possible ways to make P true, proving all those case-wise conditional statements is equivalent to proving $P \to Q$.
- Another way to see that this strategy works:

  Because $P \equiv P_1 \vee P_2 \vee \cdots \vee P_n$, it follows that

$$(P_1 \to Q) \wedge (P_2 \to Q) \wedge \cdots \wedge (P_n \to Q) \equiv P \to Q$$

Definition. Let $n \in \mathbb{Z}$ and let d be a nonzero integer. We say that d **divides** n if there exists an integer k such that $n = kd$. It means the **remainder** of n divided by d is 0.

Fact. Suppose $d \geq 1$. Then there exist unique integers k and r such that $n = kd + r$ and $0 \leq r < d$. We call r the **remainder** of n divided by d. *If d divides n, remainder is 0: n = kd + 0.

Notation. If d divides n, then we write $d|n$. If d does not divide n, then we write $d \nmid n$

Ex. $5|10$ "5 divides 10" because $10 = 2(5)$ and $2 \in \mathbb{Z}$.

Ex. $2|6$ "2 divides 6" because $6 = 3(2)$ and $3 \in \mathbb{Z}$.

Ex. $10 \nmid 13$ "10 does not divide 13" because $13 = (1)(10) + 3$ ← a remainder $r = 3$ with $0 < r < 10$

Ex. $8 \nmid 7$ "8 does not divide 7" because $7 = (0)(8) + 7$ ← a remainder $r = 7$ with $0 < r < 8$

Example 8.1. Prove the following theorem:

Theorem. Let n be an integer. If $3 \mid n^2$, then $3 \mid n$.

$P \rightarrow Q$

To prove $P \rightarrow Q$ we will use an indirect proof

Why not try proving $P \rightarrow Q$ with direct strategy?
Assume P is T. ie assume $3 \mid n^2$

Then $n^2 = 3k$ for some $k \in \mathbb{Z}$
$\Rightarrow n = \pm\sqrt{3k}$
this is not helping us to establish whether $3 \mid n$...
Fine We'll try a different strategy

We will prove $\neg Q \rightarrow \neg P$ (which is $\equiv P \rightarrow Q$)

$\neg Q$: $3 \nmid n$. (goal will be to show $\neg P$: $3 \nmid n^2$).

Proof. Let n be an integer.
Assume $\neg Q$ is True. ie Assume $3 \nmid n$.

Then, there are 2 possibilities for the remainder of n divided by 3:

Case 1 • remainder is 1: ie $n = 3k+1$ for some $k \in \mathbb{Z}$, or

Case 2 • remainder is 2: ie $n = 3k+2$ for some $k \in \mathbb{Z}$

Case 1 Assume $n = 3k+1$ for some integer $k \in \mathbb{Z}$.

Then $n^2 = (3k+1)^2$
$= 9k^2 + 6k + 1$
$= 3[3k^2 + 2k] + 1$
$= 3\ell + 1$ where $\ell = 3k^2 + 2k$. So $\ell \in \mathbb{Z}$.

$\therefore$ in this case, the remainder of n^2 divided by 3 is 1
$\therefore$ 3 does not divide n^2 in this case (so $\neg P$ is T in this case).

Case 2 Assume $n = 3k+2$ for some integer $k \in \mathbb{Z}$.

Then $n^2 = (3k+2)^2$
$= 9k^2 + 12k + 4$
$= 9k^2 + 12k + 3 + 1$
$= 3[3k^2 + 4k + 1] + 1$
$= 3\ell + 1$ where $\ell = 3k^2 + 4k + 1$. So $\ell \in \mathbb{Z}$

$\therefore$ in this case, the remainder of n^2 divided by 3 is 1
$\therefore$ 3 does not divide n^2 in this case (so $\neg P$ is T in this case).

In both possible cases where $\neg Q$ is T, we proved that $\neg P$ must also be T.
Thus, we have proved $\neg Q \rightarrow \neg P$ (by cases).

Since $\neg Q \rightarrow \neg P \equiv P \rightarrow Q$, it means we proved $P \rightarrow Q$

PROOF BY CONTRADICTION

To prove a statement, such as P, using a PROOF BY CONTRADICTION, we will

- Assume $\neg P$ is true (equivalently, assume P is false).
- Then, step-by-step, show contradiction always follows from $\neg P$.

Remark 8.2. A **proof by contradiction** is akin to the truth tree method of putting $\neg P$ at the root and discovering that all paths die (meaning lead to contradictions). This tells us that $\neg P$ can never be true, which is a way to show that P must always be true.

Example 8.3. On The Island of Knights and Knaves, you meet three inhabitants A, B, and C.

A says "B is a knave"

C says "A and B are of opposite types."

Use a **proof by contradiction** to prove that C is a knight.

Propostion to be proved: P: "C is a Knight."

For the proof by contradiction, we want to prove $\neg P \rightarrow F$

Proof.

First step: Assume $\neg P$ is true. i.e. Assume C is a Knave.

Then, C's statement must be false (by def. of a Knave of The Island)

This means A and B must be of the same type

Case 1 (both Knights)

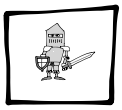
- Assume A and B are both Knights. Then A's statement "B is a Knave" would be False ↯ (this contradicts that A is a Knight)

Case 2 (both Knaves)

- Assume A and B are both Knaves. Then A's statement "B is a Knave" would be True ↯ (this contradicts that A is a Knave)

Since our assumption that C was a Knave leads to contradiction in all possible cases, we must be wrong about C.

∴ C must be a Knight



PROOF OF EQUIVALENCE

To prove a statement, such as $P \leftrightarrow Q$, using a PROOF OF EQUIVALENCE, we will

- Prove the conditional statement $P \to Q$, and
- Prove the converse $Q \to P$.

Remark 8.4. Recall (from one of the Biconditional Laws) that

$$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$$

Thus, a Proof of Equivalence simply takes care of each direction of the biconditional statement individually. To prove $P \to Q$ and $Q \to P$, we must use an appropriate strategy (ex. direct, indirect, by contradiction, by cases).

Example 8.5. Give a **proof of equivalence** of the following theorem:

Theorem. Let m and n be integers. Then $m^2 = n^2$ if and only if $m = n$ or $m = -n$.

P $\leftrightarrow$ Q

To prove $P \leftrightarrow Q$ we use a proof of equivalence.
We will prove $P \to Q$ and its converse $Q \to P$.

Proof. Let m and n be integers.

($\Rightarrow$) To prove $P \to Q$ we will use a direct proof.
Assume P is T. ie Assume $m^2 = n^2$.
Then $m^2 - n^2 = 0$
$\Rightarrow (m-n)(m+n) = 0$
$\Rightarrow m = n$ OR $m = -n$. $\therefore$ Q is T so we have proved $P \to Q$.

($\Leftarrow$) To prove $Q \to P$, we will use a proof by cases:

Q: $\underbrace{m=n}_{Q_1}$ or $\underbrace{m=-n}_{Q_2}$
$\underbrace{Q_1 \vee Q_2}_{Q}$

We will prove $(Q_1 \vee Q_2) \to P$ by proving $Q_1 \to P$ and $Q_2 \to P$.

Case 1. We will prove $Q_1 \to P$ with a direct proof.
Assume Q_1 is T. ie Assume $m = n$.
Then $m^2 = n^2$ $\therefore$ P is T. so we proved $Q_1 \to P$.

Case 2. We will prove $Q_2 \to P$ with a direct proof.
Assume Q_2 is T. i.e. Assume $m = -n$.
Then $m^2 = (-n)^2 = n^2$ ∴ P is T. so we proved $Q_2 \to P$.

Together, the cases prove $Q \to P$.

Since $P \to Q$ and $Q \to P$ are both True,
we have proved that $P \leftrightarrow Q$ (i.e. the theorem) is True

■

Exercise 8.6. Give a proof of equivalence of the following theorem:

Theorem. Let n be a positive integer. Then $3 \mid n^2$ if and only if $3 \mid n$.

hint: we already proved $P \to Q$ in Example 8.1. Now prove $Q \to P$.

VACUOUS PROOF

To prove a statement, such as $P \to Q$, using a VACUOUS PROOF, we will

- Prove the premise P is false.
- Then, $P \to Q$ is "vacuously true" because $P \to Q \equiv \mathbf{F} \to Q \equiv \mathbf{T}$.

Example 8.7. For each integer n, define the proposition: $P(n)$: If $n > 1$, then $n^2 > n$.
Prove $P(0)$ is true.

P(0): "If $0 > 1$, then $0^2 > 0$."

Since the premise "$0 > 1$" is False, the entire conditional statement is vacuously True. ■

TRIVIAL PROOF

To prove a statement, such as $P \to Q$, using a TRIVIAL PROOF, we will

- Prove the conclusion Q is true.
- Then, $P \to Q$ is "trivially true" because $P \to Q \equiv P \to \mathbf{T} \equiv \mathbf{T}$.

Example 8.8. Using the proposition $P(n)$ defined in Example 8.7, prove $P(-2)$ is true.

P(-2): "If $-2 > 1$, then $(-2)^2 > -2$."

Since the conclusion "$(-2)^2 > -2$ is True, the entire conditional statement is trivially true. ■

By Contradiction vs. Indirect (By Contraposition)

To prove a conditional statement, such as $P \to Q$, using a Proof by Contradiction, we will

- Assume the entire conditional statement is False, that is, assume $\neg(P \to Q)$ is True. Equivalently, we assume $P \wedge \neg Q$ is true.
- Then, step-by-step, we show that contradiction always follows when we assume both P and $\neg Q$ are true.

In contrast, if we prove $P \to Q$ using an Indirect Proof (by Contraposition), we will

- Assume $\neg Q$ is true.
- Then, prove that $\neg P$ must follow from $\neg Q$.

Example 8.9. Prove the following theorem in two ways:

i. By Contradiction.

ii. With an Indirect Proof (by Contraposition).

Theorem. Let n be an integer. If $\underbrace{n^3+5 \text{ is odd}}_{P}$, then $\underbrace{n \text{ is even}}_{Q}$.

$\neg Q$: n is odd.

i) To prove $P \to Q$ by contradiction we assume $\neg(P \to Q) \equiv P \wedge \neg Q$ is True

ie Assume P is True and assume $\neg Q$ is True:

Proof: Let n be an integer.

Assume n^3+5 is odd and assume n is odd.

Since n^3+5 is odd, there exists an integer k such that

$n^3+5 = 2k+1$

Since n is odd, there exists an integer m such that

$n = 2m+1$.

$\therefore 5 = 2k+1-n^3 = 2k+1-(2m+1)^3$

$= 2k+1-\left((2m)^3+3(2m)^2+3(2m)+1\right)$

$= 2k+1-\left(8m^3+12m^2+6m+1\right)$

$= 2k-8m^3-12m^2-6m$

$= 2\left[k-4m^3-6m^2-3m\right]$

$= 2l$ for $l = k-4m^3-6m^2-3m$

Thus $l \in \mathbb{Z}$.

Therefore 5 is even ↯ (contradicting the fact that $5 = 2(2)+1$ is definitely odd).

$\therefore$ Our assumption that $\neg(P \to Q)$ is True led to contradiction. $\therefore P \to Q$ must be True.

ii) To prove $P \to Q$ with an indirect proof, we will prove $\neg Q \to \neg P$.

Proof. Let n be an integer. $\neg Q$: n is odd $\neg P$: n^3+5 is even.

Assume $\neg Q$ is T. ie Assume n is odd. (goal will be to prove $\neg P$ follows from $\neg Q$).
Then $n = 2k+1$ for some $k \in \mathbb{Z}$.

Thus, $n^3+5 = (2k+1)^3+5$

$= 8k^3+12k^2+6k+1+5$

$= 2[4k^3+6k^2+3k+3]$

$= 2m$ for $m = 4k^3+6k^2+3k+3$

so $m \in \mathbb{Z}$

$\therefore n^3+5$ is even by def. ie $\neg P$ is True. We proved $\neg Q \to \neg P$ which is $\equiv P \to Q$ ■

Proof by Contradiction of the Existence of an Irrational Number

Definition. An real number x is called **rational** if $x = \frac{m}{n}$ for some integers m and n such that $n \neq 0$. A real number x that is not rational is called **irrational.**

Example 8.10. Give a **proof by contradiction** of the following theorem:

Theorem. $\underbrace{\sqrt{2} \text{ is irrational.}}_{P}$ $\neg P$: "$\sqrt{2}$ is rational."

Proof.
Assume $\neg P$ is T i.e. Assume $\sqrt{2}$ is rational.

Then, by definition of rational, $\sqrt{2} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}, n \neq 0$.

Note. We may assume that m and n have no common divisors other than ± 1.

Why? If m and n did have common divisors, then we could factor and cancel all such factors from the numerator and denominator until no common factors (other than ± 1) remained.

↳ Let's just assume that we already did all possible cancellations of all common factors of numerator/denominator ✓

Recall the first Theorem we proved (Example 7.1) but here we state it in its contrapositive form:

Thm 7.1 If m^2 is an even integer, then m is even.

Okay, so $\sqrt{2} = \frac{m}{n}$ and m, n have no common (integer) factors other than ± 1.

$\Rightarrow (\sqrt{2})^2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2}$ Thus $2 = \frac{m^2}{n^2}$ and so $m^2 = 2n^2$

Above we just proved m^2 is even since $m^2 = 2n^2$.

$\therefore$ by Thm. 7.1, it follows that m must be an even integer.

$\therefore$ $m = 2\ell$ for some integer ℓ (by def. of even)

Now, go back to our equation $2n^2 = m^2$

and sub. in $m = 2\ell$: $2n^2 = (2\ell)^2 = 4\ell^2$

divide both sides by 2: $n^2 = 2\ell^2$ ← thus n^2 is even

Apply Thm. 7.1 again! (this time to n^2) Because n^2 is even, n must be even.

Now we have arrived at a contradiction! Why? What contradiction?

Assuming $\sqrt{2}$ is rational, we got $\sqrt{2} = \frac{m}{n}$ where we made sure that m and n had no common factors other than ± 1.

Then, it followed that m is even and n is even which means m and n both have 2 as a common factor ⚡

Conclusion: Assuming $\neg P$ leads to contradiction

ie Assuming P is False leads to contradiction

$\therefore$ P must be True i.e. $\sqrt{2}$ is irrational ■

STUDY GUIDE

Important terms and concepts:

- ◇ Proof strategies: Proof by Cases Proof by Contradiction Proof of Equivalence Vacuous Proof Trivial Proof

Exercises	Sup.Ex. §3 # 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 Rosen §1.7 # 1, 2, 3, 6, 9, 13, 17, 18, 19, 24, 25 27, 29, 33, 40, 41 Rosen §1.8 # 5, 9 §4.1 # 1, 2, 5, 7, 9