# 7. Proof Strategies

- A **theorem** is a mathematical statement that is true.
- The statement of a theorem can be an atomic proposition

**Ex.** $\sqrt{2}$ is irrational.

- The statement of a theorem is often in the form of a logical argument (a set of premises that imply some conclusion), which, in its simplest form is a conditional statement $P \to Q$.

**Ex.** If $n$ is an odd integer, then $n^2$ is an odd integer.

- The premises of a mathematical argument can be a conjunction of several **axioms** (assumptions accepted without proof), new or known definitions, as well as other previously proved theorems.

**Some Remarks:**

- In propositional logic, the variables only have two truth values (**T** or **F**). We could (with enough time), check all possible truth assignments to solve our problems or prove our claims.
- In mathematical proofs, the variables can represent numbers and other more complicated mathematical objects, each having specific definitions and properties, or infinitely many possibilities.
- We will need to make use of some math (addition, subtraction, multiplication, division, real numbers, integers, rational numbers, etc...) **and** reasoning in words.
- To get some practice writing proofs, we will prove fairly simple "facts" of math. In general, the "theorems" we will prove in MAT1348 are not themselves very important... we just need some material to practice with.
- What is important is understanding the †strategy of your proof, that it is correct, and **that anyone else who reads your proof will understand your reasoning, and see at each step why your claims are logical and correct!**

⇒ Writing a proof is a bit like writing a recipe. You've baked a cake and you want to write down instructions so that others can bake the same cake you did.

☆☆☆ Make sure to clearly indicate what you are assuming vs. what you are proving.

It is not the marker's job to fill in the gaps of your proof (even if they seem "obvious")

Ex.

| ? $x = m+1$ ? <br> $x \in \mathbb{Z}$   $x$ even   $m$ odd ? ? | Let $x \in \mathbb{Z}$, and let $m = x-1$ <br> Assume $x$ is even. <br> Then $m$ must be odd... | Let $m \in \mathbb{Z}$, and let $x = m+1$. <br> Assume $m$ is odd. <br> Then $x$ must be even... |
|---|---|---|

† For now, our proof-writing practice will seem a bit like painting-by-numbers. It's a starting point. Later on, you will be free to prove (or read proofs of) more interesting mathematical results, which involve more creativity and original thought, but which will nonetheless have a logical foundation.

*These notes are solely for the personal use of students registered in MAT1348.

| NAME OF STRATEGY | PROPOSITION TO PROVE | STRATEGY OF PROOF |
|---|---|---|
| **Direct Proof** | $P \to Q$ | First step: Assume P is True<br>Then prove that Q being true must follow from P. |
| **Indirect Proof**<br><br>**(Proof by Contraposition)** | $P \to Q$<br>$\equiv \neg Q \to \neg P$ | • Prove $\neg Q \to \neg P$ directly (because $\neg Q \to \neg P \equiv P \to Q$)<br>First step: • Assume $\neg Q$ is True (i.e. Assume Q is False)<br>Then prove that $\neg P$ being true must follow from $\neg Q$ |
| **Proof by Contradiction** | $P$<br>(P could be a compound proposition such as $X \to Y$) | First step: Negate P entirely and assume $\neg P$ is True.<br>Then prove that contradiction always follows from $\neg P$ $\therefore$ P must be True |
| **Proof by Cases** | $(P_1 \vee \cdots \vee P_k) \to Q$ | We prove $(P_1 \vee P_2 \vee \cdots \vee P_k) \to Q$ by proving each of<br>$P_1 \to Q$, $P_2 \to Q$, $\ldots$, $P_k \to Q$ |
| **Proof of Equivalence** | $P \leftrightarrow Q$ | Prove both<br>$P \to Q$ and its converse $Q \to P$<br>because $P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$ |
| **Vacuous Proof** | $P \to Q$ | Simply prove P is False<br>because it will mean<br>$P \to Q \equiv F \to Q \equiv T$ |
| **Trivial Proof** | $P \to Q$ | Simply prove Q is True<br>because it will mean<br>$P \to Q \equiv P \to T \equiv T$ |

$P \to Q$

premise, conclusion

- if $P$, then $Q$
- $P$ only if $Q$
- $Q$ if $P$
- $P$ is a sufficient condition for $Q$
- $Q$ is a necessary condition for $P$

| $P$ | $Q$ | $P \to Q$ | $\neg Q$ | $\neg P$ | $\neg Q \to \neg P$ |
|---|---|---|---|---|---|
| T | T | T | F | F | T |
| T | F | F | T | F | F |
| F | T | T | F | T | T |
| F | F | T | T | T | T |

In a direct proof of $P \to Q$, we are proving that this row cannot happen.

- if $P$ is F, then $P \to Q$ is vacuously true.
- if $Q$ is T, then $P \to Q$ is trivially true.

- Thus, the only chance for $P \to Q$ to be F is when $P$ is T.
- So, the direct proof strategy is to assume $P$ is T, and then show (using math, definitions, other known theorems, etc) that $Q$ must be true.

In an indirect proof of $P \to Q$, we are proving that this row cannot happen.

- if $\neg Q$ is F, then $\neg Q \to \neg P$ is vacuously true.
- if $\neg P$ is T, then $\neg Q \to \neg P$ is trivially true.

- Thus, the only chance for $\neg Q \to \neg P$ to be F is when $\neg Q$ is T.
- So, the indirect proof strategy is to assume $\neg Q$ is T, and then show (using math, definitions, other known theorems, etc) that $\neg P$ must be true.
- Finally, since $\neg Q \to \neg P \equiv P \to Q$, the indirect proof is a way to prove $P \to Q$.

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

- Assume $P$ is true.
- Then, step-by-step, show that $Q$ must follow from $P$.

**Definition.** An integer $n$ is called **even** if $n = 2k$ for some integer $k$, and $n$ is called **odd** if $n = 2m + 1$ for some integer $m$.

**Example 7.1.** Give a **direct proof** of the following theorem:

**Theorem.** Let $n$ be an integer. If $\underbrace{n \text{ is odd}}_{P}$, then $\underbrace{n^2 \text{ is odd}}_{Q}$. $P \to Q$

Proof. Let $n$ be an integer.

Assume $P$ is T. ie Assume $n$ is odd (goal: show $Q$ must be T).

Then, by def. of odd, $n = 2k+1$ for some integer $k$.

Consequently, $n^2 = (2k+1)^2$

$$= 4k^2 + 4k + 1$$

$$= 2[\underbrace{2k^2 + 2k}] + 1$$

$$= 2 \times m + 1 \quad \text{for } m = 2k^2 + 2k$$

(using a different variable than $k$)

Since $k \in \mathbb{Z}$, it follows that $m$ is also an integer.

Thus, by def. of odd, $\underbrace{n^2 \text{ is odd}}_{\text{ie } Q \text{ is T.}}$.

$\therefore P \to Q$ is true. ■

---

Next Indirect proof strategy / Proof by Contraposition

Ex. Contrapositive of Theorem from Ex. 7.1: $\boxed{\text{If } n^2 \text{ is even, then } n \text{ is even.}}$

We proved the theorem from Ex. 8.1 but it is logically equivalent to its contrapositive.

Think about trying to prove this restatement of the same theorem with a direct proof strategy:

Assume $n^2$ is even. Then $n^2 = 2k$ for some integer $k$ (def of even)
and $k$ must be $\geq 0$ because $n^2 \geq 0$.

Thus $n = \pm\sqrt{2k}$ ← while this is true, it's not helping us to see that $n$ must be even...

## Indirect Proof (Proof by Contraposition)

To prove a conditional statement, such as $P \to Q$, using an Indirect Proof, also called a Proof by Contraposition, we will

- Assume $\neg Q$ is true (equivalently, assume $Q$ is false).
- Then, step-by-step, show that $\neg P$ must follow from $\neg Q$.

**Remark 7.2.** Recall that $P \to Q \equiv \neg Q \to \neg P$.

Thus, an indirect proof of $P \to Q$ is simply a direct proof of the **contrapositive** conditional statement $\neg Q \to \neg P$

**Example 7.3.** Give an **indirect proof (proof by contraposition)** of the following theorem:

**Theorem.** Let $n$ be an integer. If $\underbrace{5n + 4 \text{ is odd}}_{P}$, then $\underbrace{n \text{ is odd}}_{Q}$.

$P \longrightarrow Q$

$\neg P$: $5n+4$ is even. $\neg Q$: $n$ is even

For the indirect proof strategy, we want to prove $\neg Q \to \neg P$.

proof. Let $n$ be an integer.

Assume $\neg Q$ is T.

ie Assume $n$ is even. (goal: show $\neg P$ must be true)

Then, by def. of even, we have $n = 2k$ for some integer $k \in \mathbb{Z}$.

$$\begin{aligned} \text{Thus, } 5n+4 &= 5(2k)+4 \\ &= 10k+4 \\ &= 2(5k+2) \\ &= 2m \text{ where } m = 5k+2, \text{ hence } m \text{ is an integer.} \end{aligned}$$

Thus, $5n+4$ is also even (by def. of even).

$\therefore \neg P$ is True.

So we proved $\neg Q \to \neg P$ which is $\equiv P \to Q$ ∎

## Study Guide

- Proof Strategies: direct proof of $P \to Q$ versus indirect proof of $P \to Q$

| | |
|---|---|
| Exercises | Sup.Ex. §3 # 7, 8, 9<br>Rosen §1.7 # 1, 2, 3, 4, 5, 6, 7, 13, 17, 18, 19a, 20a |