7. Proof Strategies

Arguments

- ◇ An argument is a claim that a conclusion C is true *whenever* all premises in a given set are true.
- ◇ We can view an argument as a conditional statement of the following form:

$$(P_1 \wedge \cdots \wedge P_k) \rightarrow C$$

- ◇ An argument is called **valid** if the conditional statement $(P_1 \wedge \cdots \wedge P_k) \rightarrow C$ is a tautology.
- ◇ The only situation in which a conditional statement can be false is when the overall "big" premise $P_1 \wedge \cdots \wedge P_k$ is true but the conclusion C is false.

The only situation in which the argument can be false:

$(P_1 \wedge \cdots \wedge P_k) \rightarrow C$

$T \rightarrow F$

∴ argument is invalid if and only if there exists at least one way in which all premises are T but the conclusion is F.

When one or more of the premises is false, the argument will be of the form $\mathbf{F} \rightarrow C \equiv \mathbf{T}$.

This means that in order to verify whether or not an argument $(P_1 \wedge \cdots \wedge P_k) \rightarrow C$ is **valid**, we need only consider situations in which *all* premises are true, and we must then verify that the conclusion is true in all such situations.

Suppose we discover a situation in which all premises are true but the conclusion is false. Then we would know that the argument is **invalid** because there is at least one situation in which it can be false.

MATHEMATICAL 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 $P \rightarrow Q$.

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.

---

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

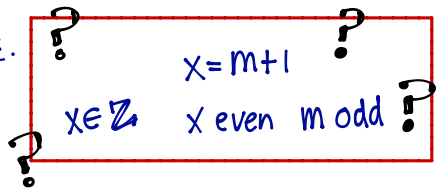
Some Remarks:

- ◇ In propositional logic, we dealt with variables which have two truth values (**T** or **F**), and a small handful of logical connectives. With a finite number of propositional variables, we could (with enough time), check all possible truth assignments to solve our problems or prove our claims.
- ◇ In mathematical proofs, we will deal with numbers and other more complicated mathematical objects, each having specific definitions and properties.
- ◇ We will need to make use of some math (addition, subtraction, multiplication, division, real numbers, integers, rational numbers, etc...) **and** reasoning in words.
- ◇ Mathematical proofs are written in words, using some notation to make the writing more understandable, and with some equations, depending on the content of the proof.
- ◇ To get some practice writing proofs, we will prove fairly simple "facts" of math.
- ◇ 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!**

☆☆☆ 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.



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

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

- ◇ In general, the "theorems" we will prove in MAT1348 are not themselves very important... we just need some material to practice with.
- ◇ 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.

Some Notation For Important Sets of Numbers

Natural Numbers. $\mathbb{N}$ $\quad 0, 1, 2, 3, \ldots$

Integers. $\mathbb{Z}$ $\quad \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$

Rational Numbers. $\mathbb{Q}$ $\quad \left\{ \frac{m}{n} \ : \ m, n \in \mathbb{Z}, n \neq 0 \right\}$

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

CONDITIONAL STATEMENTS

$P \to Q$

premise → P, conclusion → Q

- 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→Q	¬Q	¬P	¬Q→¬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→Q, we are proving that this row cannot happen.

- if P is F, then P→Q is vacuously true.
- if Q is T, then P→Q is trivially true.

- Thus, the only chance for P→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→Q, we are proving that this row cannot happen.

- if ¬Q is F, then ¬Q→¬P is vacuously true.
- if ¬P is T, then ¬Q→¬P is trivially true.

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

DIRECT PROOF

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 n is odd, then n^2 is odd.

P → 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, $n^2 = (2k+1)^2$

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

$= 2[2k^2 + 2k] + 1$

$= 2 \times m + 1$ 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, n^2 is odd.

ie Q is T.

∴ P → Q is true. ▨

Next Indirect proof strategy / Proof by Contraposition

Ex. Contrapositive of Theorem from Ex. 7.1: If n^2 is even, then n 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 ≥ 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 $5n + 4$ is odd, then n is odd.

P → Q

¬P: 5n+4 is even. ¬Q: n is even

For the indirect proof strategy, we want to prove ¬Q→¬P.

proof. Let n be an integer.

Assume ¬Q is T.

ie Assume n is even. (goal: show ¬P must be true)

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

Thus, $5n+4 = 5(2k)+4$
$= 10k+4$
$= 2(5k+2)$
$= 2m$ where $m=5k+2$, hence m is an integer.

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

∴ ¬P is True.

So we proved ¬Q→¬P which is ≡ P→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 Rosen §1.7 # 1, 2, 3, 4, 5, 6, 15, 16, 17a, 18a