# Module 3: Proof Techniques

## Theme 1: Rule of Inference

Let us consider the following example.
**Example 1**: Read the following "obvious" statements:

> All Greeks are philosophers.
>
> Socrates is a Greek.
>
> Therefore, Socrates is a philosopher.

This conclusion seems to be perfectly correct, and quite obvious to us. However, we cannot justify it rigorously since we do not have any *rule of inference*. When the chain of implications is more complicated, as in the example below, a formal method of inference is very useful.

**Example 2**: Consider the following hypothesis:

1. It is not sunny this afternoon and it is colder than yesterday.
2. We will go swimming only if it is sunny.
3. If we do not go swimming, then we will take a canoe trip.
4. If we take a canoe trip, then we will be home by sunset.

From this hypothesis, we should conclude:

> We will be home by sunset.

We shall come back to it in Example 5.

The above conclusions are examples of a **syllogisms** defined as a "deductive scheme of a formal argument consisting of a major and a minor premise and a conclusion". Here what `encyclopedia.com` is to say about syllogisms:

> *Syllogism*, a mode of argument that forms the core of the body of Western logical thought. Aristotle defined syllogistic logic, and his formulations were thought to be the final word in logic; they underwent only minor revisions in the subsequent 2,200 years.

We shall now discuss **rules of inference** for propositional logic. They are listed in Table 1. These rules provide justifications for steps that lead logically to a conclusion from a set of hypotheses. Because the emphasis is on *correctness* of arguments, these rules, when written as a proposition, are **tautologies**. Recall that a tautology is a proposition that is *always* true.

**Table 1: Rules of Inference**

| *Rule of Inference* | *Tautology* | *Name* | *Explanation* |
|---|---|---|---|
| $\begin{array}{l} p \\ \hline \therefore p \lor q \end{array}$ | $p \to (p \lor q)$ | Addition | If the hypothesis is true, then the disjunction is true. |
| $\begin{array}{l} p \land q \\ \hline \therefore p \end{array}$ | $(p \land q) \to p$ | Simplification | If a conjunction of hypotheses is true, then the conclusion is true. |
| $\begin{array}{l} p \\ q \\ \hline \therefore p \land q \end{array}$ | $((p) \land (q)) \to (p \land q)$ | Conjunction | If both hypotheses are true, then the conjunction of them is true. |
| $\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array}$ | $[p \land (p \to q)] \to q$ | Modus ponens | If both hypotheses are true, then the conclusion is true. |
| $\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore \neg p \end{array}$ | $[\neg q \land (p \to q)] \to \neg p$ | Modus tollens | If a hypothesis is not true and an implication is true, then the other proposition cannot be true. |
| $\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$ | $[(p \to q) \land (q \to r)] \to p \to r$ | Hypothetical syllogism | If both implications are true, then the resulting implication is true. |
| $\begin{array}{l} p \lor q \\ \neg p \\ \hline \therefore q \end{array}$ | $[p \lor q) \land \neg p] \to q$ | Disjunctive syllogism | If a disjunction is true, and one proposition is not true, then the other proposition must be true. |

Let us start with the following proposition (cf. Table 1)

$$(p \land (p \to q)) \to q.$$

The table below shows that it is a tautology.

| $p$ | $q$ | $p \to q$ | $p \land (p \to q)$ | $(p \land (p \to q)) \to q$ |
|---|---|---|---|---|
| T | T | T | T | T |
| T | F | F | F | T |
| F | T | T | F | T |
| F | F | T | F | T |

This tautology is the basis of the rule of inference called **modus ponens** or **law of detachment** that we actually used in Example 1 to infer the above conclusion. Such a rule is often written as follows:

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q. \end{array}$$

In this notation, the hypotheses (i.e., $p$ and $p \to q$) are listed in a column, and the conclusion (i.e., $q$) below a bar, where the symbol $\therefore$ should be read as "therefore". In words, modus ponens states that if both the hypotheses are true, then the conclusion must be true. We should emphasize that the whole proposition is a tautology, whence it is true for any assignments of truth values. However, in the case of rules of inference we are mostly interested when the hypotheses are true, and make sure they imply truth.

**Example 3**: Suppose that

$$p \to q \;\equiv\; \text{if } n \text{ is divisible by } 5, \text{ then } n^3 \text{ is divisible by } 125$$

is true. Consequently, if we pick up an integer $n$ that is divisible by $5$ (say $n = 10$), then by modus ponens it follows that $n^3$ must be divisible by $125$ (in our example, indeed $n^3 = 1000$ is divisible by $125$).

We now discuss and illustrate other rules of inference. We start with the simplest one, the rule of **addition** (cf. Table 1)

$$\begin{array}{l} p \\ \hline \therefore p \vee q \end{array}$$

which states that if $p$ is true, then the conclusion $p \vee q$ must be true (by the virtue of the fact that for $p \vee q$ to be true it suffices that at least one of the proposition involved is true).

**Example 4**: Let us assume that: “it is raining now” is true. Therefore, “it is either raining or it is freezing” is true.

Consider the following inference:

It is sunny **and** raining.

**Therefore**, it is sunny now.

What rule of inference did we use? Clearly, the **simplification rule** (cf. Table 1)

$$\begin{array}{l} p \wedge q \\ \hline \therefore p \end{array}$$

since if a conjunction is true, then both propositions must be true. This rule is a tautology since $(p \wedge q) \to p$ is always true, as easy to check.

Consider the following example:

I am **not** going to ski.

If it is snowing, then I am going to ski.

From these two hypotheses, we can only conclude that: “It is not snowing”. To do it we invoke the rule of **modus tollens** that can be symbolically written as follows:

$$\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore \neg p. \end{array}$$

In other words, counterpositive $\neg q \to \neg p$ is true, if $p \to q$ is true, as we have seen in Module 1.

As a "sanity check", we may want to use common sense to verify the last rule. From the truth of $p \to q$ we infer that if $q$ is false then $p$ must be false since otherwise the implication would be false, which not the case.

**Exercise 3A**: Using the truth table (as we did above when discussing modus ponens) prove modus tollens (cf. Table 1).

**Example 5**: We will use the hypotheses in Example 2 and our rules of inference to logically obtain the conclusion. Let

$$
\begin{aligned}
p &\equiv \text{it is sunny this afternoon} \\
q &\equiv \text{it is colder than yesterday} \\
r &\equiv \text{we will go swimming} \\
s &\equiv \text{we will take a canoe trip} \\
t &\equiv \text{we will be home by sunset}
\end{aligned}
$$

Now, we construct arguments to show that our hypotheses 1-4 from Example 2 lead to the conclusion $t$. Here how it goes:

| Step | Reason | Explanation |
|---|---|---|
| 1. $\neg p \wedge q$ | Hypothesis 1 | It is not sunny this afternoon and it is colder than yesterday. |
| 2. $\neg p$ | Simplification | It is not sunny. |
| 3. $r \to p$ | Hypothesis 2 | We will go swimming only if it is sunny. |
| 4. $\neg r$ | Modus tollens from Steps 2 and 3 | We will not go swimming. |
| 5. $\neg r \to s$ | Hypothesis 3 | If we do not go swimming, then we will take a canoe trip. |
| 6. $s$ | Modus ponens from Steps 4 and 5 | We will take a canoe trip. |
| 7. $s \to t$ | Hypothesis 4 | If we take a canoe trip, then we will be home by sunset. |
| 8. $t$ | Modus ponens from Steps 6 and 7 | We will be home by sunset. |

## Theme 2: Fallacies

Fallacies arise in incorrect arguments that are based on contingencies[1] rather than on tautologies. It is important to realize it and we shall discuss three fallacies, namely, *fallacy of affirming the conclusion*, *fallacy of denying the hypothesis*, and the most important *circular reasoning*.

The **fallacy of affirming the conclusion** is based on the following proposition

$$[(p \to q) \wedge q] \to p$$

which is false when $p$ is false and $q$ is true. This fallacy was already discussed in Module 1 since it is equivalent to conclude converse $q \to p$ from $p \to q$, which we know is not true in general. In words, this fallacy says that converse implication does not follow the direct implication.

**Example 6**: Let two propositions $p$ and $q$ be given as follows:

$$\begin{aligned} p &\equiv n = 1 \bmod 3, \\ q &\equiv n^2 = 1 \bmod 3. \end{aligned}$$

In words, when the remainder of dividing $n$ by 3 is 1, then we also get remainder 1 when dividing $n^2$ by 3. It is easy to see that $p \to q$. Indeed, if $n = 1 \bmod 3$, then there exists an integer $k$ such that $n = 3k + 1$. Observe that $n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, thus $n^2 - 1 = 3(3k^2 + 2k)$ and is divisible by 3. In other words, $n^2 = 1 \bmod 3$. Let us now assume that $q$ is true, that is, $n^2 = 1 \bmod 3$. Does it imply that $p$ is true? Not necessary, since it may happen that $n = 2 \bmod 3$ (e.g., take $n = 5$ to see that $25 = 1 \bmod 3$ but $5 = 2 \bmod 3$).

**Exercise 3B**: Is the following argument valid or not? If yes, what rule of inference is being used? If not, what fallacy occurs?

> If $x$ is a real number such that $x > 1$, then $x^2 > 1$.
>
> Suppose that $x^2 > 1$. Then $x > 1$.

The **fallacy of denying the hypothesis** is based on

$$[(p \to q) \wedge \neg p] \to \neg q \tag{1}$$

which is false when $p$ is false and $q$ is true. In fact, it is not a rule of inference since the inverse $\neg p \to \neg q$ is not equivalent to $p \to q$, as we saw in Module 1.

**Example 7**: Let us use the same propositions $p$ and $q$ as in Example 6. We know that $p \to q$, that is, $n = 1 \bmod 3$ implies $n^2 = 1 \bmod 1$. Assume now that $n$ is *not* equal to 1 modulo 3. Does it imply $n^2$ is *not* equal to 1 modulo 3. No, since $n^2 = 1 \bmod 3$ not only when $n = 1 \mathbf{\ mod\ } 3$ but also $n = 2 \bmod 3$, as we saw before.

[1] Recall that a contingency is neither a tautology nor a contradiction and may be true or false.

The fallacy of **circular reasoning** or **begging the question** (or more common known as “catch 22”) occurs when during the proof we *assume* that the statement being proved is true. Of course, this leads to nowhere.

**Example 8**: Let us “prove” the following statement

> If $n^2$ is not divisible by $3$, then $n$ is not divisible by $3$.

Consider the following *incorrect* proof:

> Since $n^2$ is not divisible by $3$, hence $n^2$ cannot be equal to $3k$ for some integer $k$. Thus, if $n$ cannot be equal to $3l$ for some integer $l$, therefore, $n$ is not divisible by $3$.

It should be clear to an astute reader, then the assumption “if $n$ not equal to $3l$” is equivalent to the statement being proved, so here where the circular incorrect argument is used. We *assumed* to be true what we supposed to prove. This is of course illegal.

The rule of inference for quantified statements are summarized in Table 2. They are self-explanatory. For example, if $\forall x P(x)$, then naturally for any $c$ in the universe of discourse $P(c)$ must be true, where $P(x)$ is a predicate.

Table 2 Rules of Inference ($U$ is the universe of discourse)

| *Rule of Inference* | *Name* | *Explanation* |
|---|---|---|
| $\forall x P(x)$<br>$\therefore P(c)$ if $c \in U$ | Universal instantiation | If $P(x)$ is true for all $x$,<br>then it must be true for one, say $c$. |
| $P(c)$ for an arbitrary $c \in U$<br>$\therefore \forall x P(x)$ | Universal generalization | If $P(c)$ is true for any $c$,<br>then $P(x)$ is true for all $x$ in the universe. |
| $\exists x P(x)$<br>$\therefore P(c)$ for some $c \in U$ | Existential instantiation | If $P(x)$ is true for at least one $x$,<br>then it must be true for some $c$. |
| $P(c)$ for some $c \in U$<br>$\therefore \exists x P(x)$ | Existential generalization | If $P(c)$ is true for some $c$ in the universe,<br>then there exists $x$ such that $P(x)$ is true. |

## Theme 3: Methods of Proving Theorems

As readers already observed, theorems are statements of the form $p \to q$, thus techniques for proving implications are very important. We recall that $p \to q$ is true *unless* $p$ =true and $q$ =false. In mathematics truth can*not* imply false (otherwise will will produce a heap of half-truths, nonsense, and false statements). We shall discuss several proof techniques such as: direct proof, indirect proof, proof by contradiction, vacuous proof, trivial proof, and proof by cases.

We start with a **direct proof**. Such a proof shows, using the rule of inferences that we just learned, that if $p$ is true, then $q$ must be true. Any established mathematical fact **proved before**, axioms (facts assumed to be true at the beginning of building a theory), as well as definitions can be used to deduce the truth of the conclusion in a theorem.

**Example 9**: Let us prove the following theorem:

**Theorem 1** *If $n$ is an even integer, then $n^2$ is even. In general, $n^k$ ($k$ is a natural number) is even.*
**Proof**. We assume that $n$ is even. An even number can be represented as a product of 2 and an integer, thus, $n = 2l$, where $l$ is an integer. Then

$$\begin{aligned} n^2 &= 2^2 l^2 = 2(2l^2) = 2l_1, \\ n^k &= 2^k l^k = 2(2^{k-1} l^k) = 2l_2 \end{aligned}$$

where $l_1, l_2$ are integers, thus $n^2$ and $n^k$, $k \in \mathbf{N}$ are even numbers.

**Exercise 3C**: Using a direct proof show that the square of an odd number is odd.

In Module 1 we proved that the implication $p \to q$ is equivalent to $\neg q \to \neg p$ (the latter is called a contrapositive). Thus we can prove a direct implication $p \to q$ indirectly by showing that $\neg q \to \neg p$. This is called a **proof by contradiction**. This is also called an **indirect proof**, since one assumes that the hypothesis $p$ is true while the conclusion $q$ is false and using rules of inference we derive a *contradiction*. Recall that a contradiction is a proposition that is always false (e.g., $r \wedge \neg r$). To see that an indirect proof is equivalent to $p \to q$ we use truth table (cf. Table 3) to prove the following equivalence

$$p \to q \quad \equiv \quad p \wedge \neg q \to r \wedge \neg r. \tag{2}$$

Thus to prove $p \to q$ it suffices to assume that $p$ is true and $q$ is false, and show that this leads to a contradiction $r \wedge \neg r$.

Table 3: The truth table of (1).

| $p$ | $q$ | $r$ | $p \to q$ | $p \wedge \neg q$ | $r \wedge \neg r$ | $p \wedge \neg q \to r \wedge \neg r$ |
|---|---|---|---|---|---|---|
| T | T | T | T | F | F | T |
| T | T | F | T | F | F | T |
| T | F | T | F | T | F | F |
| T | F | F | F | T | F | F |
| F | T | T | T | F | F | T |
| F | T | F | T | F | F | T |
| F | F | T | T | F | F | T |
| F | F | F | T | F | F | T |

**Example 10**: We prove the following lemma using an indirect proof.

**Lemma 2** *If* $5n + 2$ *is odd, then* $n$ *is odd.*

**Proof**. We use an indirect proof, that is, we assume that the hypothesis (i.e., " $n$ is odd") is false, and will prove that this will lead to $5n + 2$ being even, which will contradict the hypothesis. Since we assume $n$ is even, hence there exists an integer, say $k$, such that $n = 2k$ (this is the definition of even numbers!) for some integer $k$. Then

$$5n + 2 = 5(2k) + 2 = 10k + 2 = 2(5k + 1) = 2k_1$$

where $k_1 = 5k + 1$ is an integer since $k$ is an integer. Hence $5n + 2$ is even, which contradicts the hypothesis, and therefore by a contrapositive argument we prove the lemma.

**Example 11**: The next theorem is one of the most famous result known already to Ancient Greeks. We recall that a number $x$ is rational if it is a ratio of two integers. If $x$ cannot be represented as such a ratio, then $x$ is called irrational.

**Theorem 2** *The number* $\sqrt{2}$ *is irrational.*

**Proof**. We prove it by contradiction assuming that $\sqrt{2}$ is rational. So we assume that $\neg q$ is true, where

$$q \equiv \sqrt{2} \text{ is irrational}.$$

If $\sqrt{2}$ is rational, then there are two integers, say $k$ and $m$ such that

$$\sqrt{2} = \frac{k}{m}$$

*and* $k$ and $m$ have *no* common factors (so the fraction $k/m$ is in the lowest terms and cannot be any further reduced; like $\frac{1}{2}$ but not like $\frac{3}{6}$). Now, square both sides of the above to yield

$$2 = \frac{k^2}{m^2},$$

which further leads to

$$2m^2 = k^2. \tag{3}$$

The latter implies that $k^2$ must be even (since if $k$ is not even, then $k = 2l + 1$ for some integer $l$ and $k^2 = 4l^2 + 2l + 1$ is odd), hence $k$ must be even. Let then $k = 2n$, thus from (2) we arrive at

$$2m^2 = 4n^2$$

which implies

$$m^2 = 2n^2.$$

Therefore, $m^2$ is even, and also $m$ must be even (by the same argument as above). In conclusion, we prove that $k$ and $m$ are even. This is the desired contradiction since we assume that

$$r \equiv k \text{ and } m \text{ have no common factor},$$

while we prove that

$$\neg r \equiv k \text{ and } m \text{ have a common factor equal to } 2.$$

We have shown that $\neg q = \sqrt{2}$ is not irrational leads to a contradiction $r \wedge \neg r$, thus $\sqrt{2}$ must be irrational.

If $p$ in $p \to q$ is false, then the implication is true doesn't matter what is the value of $q$ since an implication is false *only* if true implies false (see Module 1). Consequently, if we can show that $p$ is false, then a proof, called a **vacuous proof**, of $p \to q$ is given.

**Example 12**: Consider the following predicate $P(n)$:

> If $n > 1$, then $2n + 2$ is even.

Let us consider now $P(0)$, that is, we want to know if $P(0)$ is true or not. But for $n = 0$ the hypothesis $0 > 1$ is false, thus $P(0)$ must be automatically true.

If in the implication $p \to q$ we know that $q$ is true, then the implication must be true, and this leads to a **trivial proof**.

**Example 13**: Let $P(n)$ be the proposition:

> If $a$ and $b$ are positive integers such that $a \geq b$, then $a^n \geq b^n$.

Since trivially $a^0 = 1 \geq b^0 = 1$, the implication is true for $n = 0$ (because $1 = 1$ as we have just shown).

Finally, the implication

$$(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$$

is equivalent to

$$(p_1 \to q) \vee (p_2 \to q) \vee \cdots \vee (p_n \to q).$$

We can use the latter to prove a theorem. Such an argument is called a **proof by cases**.

**Example 14**: We want to prove the following theorem.

**Theorem 4** *If $n$ is an integer not divisible by $3$, then*

$$n^2 = 1 \bmod 3, \tag{4}$$

*that is, when dividing $n^2$ by $3$ we obtain a remainder equal to $1$.*

**Proof**. The proposition $p$: "$n$ is not divisible by 3" is equivalent to:

$$\begin{aligned} p_1 &\equiv n = 1 \bmod 3, \\ p_2 &\equiv n = 2 \bmod 3 \end{aligned}$$

since if $n$ is not divisible by 3, then there is either a remainder equal to $1$ or to $2$. Thus our theorem is equivalent to prove that $p_1 \vee p_2 \to q$ where

$$q \equiv n^2 = 1 \bmod 3.$$

The last statement is exactly what we need to prove. We shall use the proof by cases.

We first assume that $p_1$ is true, that is, $n = 3k + 1$ for some integer $k$. Clearly,

$$n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1,$$

thus $n^2 = 1 \bmod 3$.

Now, we consider the second case, that is, we assume $p_2$ is true, which amounts to $n = 3l + 2$ for an integer $l$. Then

$$n^2 = (3l + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1.$$

Therefore, $n^2$ when divided by 3 gives the remainder $1$ (i.e., $n^2 = 1 \mod 3$).

In summary, we prove $p_1 \to q$ and $p_2 \to q$, therefore, $p_1 \vee p_2 \to q$, which completes the proof by cases.