3. Proofs

3.1. Mathematical Systems, Proofs. A *Mathematical System* consists of:

1. *Axioms*: propositions that are assumed true.
2. *Definitions*: used to create new concept from old ones.
3. *Undefined terms*: corresponding to the primitive concepts of the system (for instance in set theory the term "set" is undefined).

A *theorem* is a proposition that has been proved to be true. An argument that establishes the truth of a proposition is called a *proof*.

Example: Prove that if $x > 2$ and $y > 3$ then $x + y > 5$.

Answer: Assuming $x > 2$ and $y > 3$ and adding the inequalities term by term we get: $x + y > 2 + 3 = 5$.

That is an example of *direct proof*. In a direct proof we assume the hypothesis together with axioms and other theorems previously proved and we derive the conclusion from them.

Proof by Contradiction. In a *proof by contradiction* or (*Reductio ad Absurdum*) we assume the hypothesis and the negation of the conclusion, and try to derive a *contradiction*, i.e., a proposition of the form $r \wedge \overline{r}$.

Example: Prove by contradiction that if $x+y > 5$ then either $x > 2$ or $y > 3$.

Answer: We assume the hypothesis $x + y > 5$. From here we must conclude that $x > 2$ or $y > 3$. Assume to the contrary that "$x > 2$ or $y > 3$" is false, so $x \leq 2$ and $y \leq 3$. Adding those inequalities we get $x \leq 2 + 3 = 5$, which contradicts the hypothesis $x + y > 5$. From here we conclude that the assumption "$x \leq 2$ and $y \leq 3$" cannot be right, so "$x > 2$ or $y > 3$" must be true.

A related proof is the *proof by contrapositive*, i.e., instead of proving $p \to q$ we prove the contrapositive $\overline{q} \to \overline{p}$.

3.2. Arguments, Rules of Inference. An *argument* is a sequence of propositions $p_1, p_2, \ldots, p_n$ called *hypothesis* (or *premises*)

followed by a proposition q called *conclusion*. An argument is usually written:

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ \underline{p_n} \\ \therefore \quad q \end{array}$$

or

$$p_1, p_2, \ldots, p_n / \therefore q$$

The argument is called *valid* if q is true whenever $p_1, p_2, \ldots, p_n$ are true; otherwise it is called *invalid*.

Rules of inference are certain simple arguments known to be valid and used to make a proof step by step. For instance the following argument is called *modus ponens* or *law of detachment*:

$$\begin{array}{l} p \to q \\ \underline{p} \\ \therefore \quad q \end{array}$$

In order to check whether it is valid we must examine the following truth table:

p	q	$p \to q$	p	q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	F

If we look now at the rows in which both $p \to q$ and p are true (just the first row) we see that also q is true, so the argument is valid.

Other rules of inference are the following:

1. *Modus Ponens* or *Rule of Detachment*:

$$\begin{array}{l} p \to q \\ \underline{p} \\ \therefore \quad q \end{array}$$

2. *Modus Tollens*:

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

3. *Addition*:

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

4. *Simplification*:

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

5. *Conjunction*:

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

6. *Hypothetical Syllogism*:

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

7. *Disjunctive Syllogism*:

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

Arguments are usually written using three columns. Each row contains a label, a statement and the reason that justifies the introduction of that statement in the argument. That justification can be one of the following:

1. The statement is a *premise*.
2. The statement can be derived from statements occurring earlier in the argument by using a *rule of inference*.

Example: Consider the following statements: "I take the bus or I walk. If I walk I get tired. I do not get tired. Therefore I take the bus." We can formalize this by calling B = "I take the bus", W = "I walk" and T = "I get tired". The premises are $B \vee W$, $W \to T$ and $\overline{T}$, and the conclusion is B. The argument can be described in the following steps:

step	statement	reason
1)	$W \to T$	Premise
2)	$\overline{T}$	Premise
3)	$\overline{W}$	1,2, Modus Tollens
4)	$B \vee W$	Premise
5)	$\therefore B$	4,3, Disjunctive Syllogism

3.3. Rules of Inference for Quantified Statements. We state the rules for predicates with one variable, but they can be generalized to predicates with two or more variables.

1. *Universal Instantiation.* If $\forall x\, p(x)$ is true, then $p(a)$ is true for each specific element a in the domain of discourse; i.e.:
$$\frac{\forall x\, p(x)}{\therefore\ \ p(a)}$$
For instance, from $\forall x\,(x+1 = 1+x)$ we can derive $7+1 = 1+7$.

2. *Existential Instantiation.* If $\exists x\, p(x)$ is true, then $p(a)$ is true for some specific element a in the domain of discourse; i.e.:
$$\frac{\exists x\, p(x)}{\therefore\ \ p(a)}$$
The difference respect to the previous rule is the restriction in the meaning of a, which now represents some (not any) element of the domain of discourse. So, for instance, from $\exists x\,(x^2 = 2)$ (the domain of discourse is the real numbers) we derive the existence of some element, which we may represent $\pm\sqrt{2}$, such that $(\pm\sqrt{2})^2 = 2$.

3. *Universal Generalization.* If $p(x)$ is proved to be true for a generic element in the domain of discourse, then $\forall x\, p(x)$ is true; i.e.:
$$\frac{p(x)}{\therefore\ \ \forall x\, p(x)}$$
By "generic" we mean an element for which we do not make any assumption other than its belonging to the domain of discourse. So, for instance, we can prove $\forall x\,[(x+1)^2 = x^2 + 2x + 1]$ (say, for real numbers) by assuming that x is a generic real number and using algebra to prove $(x+1)^2 = x^2 + 2x + 1$.

4. *Existential Generalization.* If $p(a)$ is true for some specific element a in the domain of discourse, then $\exists x\, p(x)$ is true; i.e.:

$$\frac{p(a)}{\therefore \quad \exists x\, p(x)}$$

For instance: from $7 + 1 = 8$ we can derive $\exists x\, (x + 1 = 8)$.

Example: Show that a counterexample can be used to disprove a universal statement, i.e., if a is an element in the universe of discourse, then from $\overline{p(a)}$ we can derive $\overline{\forall x\, p(x)}$. *Answer*: The argument is as follows:

step	statement	reason
1)	$\overline{p(a)}$	Premise
2)	$\exists x\, \overline{p(x)}$	Existential Generalization
3)	$\overline{\forall x\, p(x)}$	Negation of Universal Statement