10 Inference

In this section, we discuss the application of logic to proving theorems. In principle, every proof should be reducible to a sequence of simple logical deductions. While this is not practical for human consumption, there have been major strides toward that goal in computerized proof systems.

Modus ponens. This is an example of *direct inference*, the cornerstone of logical arguments.

PRINCIPLE OF MODUS PONENS. From p and $p \Rightarrow q$, we may conclude q.

We read this as a recipe to prove q. First we prove p, then we prove that p implies q, and finally we conclude q. Let us take a look at Table 11 to be sure. We see that modus

p	q	$(p \wedge (p \Rightarrow q))$	$\Rightarrow$	q
T	T	T T T	T	T
T	F	T F F	T	F
F	T	F F T	T	T
F	F	F F T	T	F

Table 11: The truth table for modus ponens.

ponens is indeed a tautology, that is, it is always true. Every theorem is this way, namely always true.

Other methods of direct inference. There are many other direct proof principles, all easy to verify. Some are straighforward re-interpretations of logical formulas and others use logical equivalences we have learned about. Here are but a few:

$$\begin{aligned} p \text{ and } q \quad &\text{then} \quad p \wedge q; \\ p \text{ or } q \quad &\text{then} \quad p \vee q; \\ q \text{ or } \neg p \quad &\text{then} \quad p \Rightarrow q; \\ \neg q \text{ and } p \quad &\text{then} \quad p \not\Rightarrow q; \\ p \Rightarrow q \text{ and } q \Rightarrow p \quad &\text{then} \quad p \Leftrightarrow q; \\ p \Rightarrow q \text{ and } q \Rightarrow r \quad &\text{then} \quad p \Leftrightarrow r. \end{aligned}$$

The last principle is perhaps more interesting than the others because it is the only one among the six that is not an equivalence; see Table 12.

Contrapositive. This is the first example of an *indirect inference* method.

p	q	r	$((p \Rightarrow q) \wedge (q \Rightarrow r))$	$\Rightarrow$	$(p \Rightarrow r)$
T	T	T	T T T	T	T
T	T	F	T F F	T	F
T	F	T	F F T	T	T
T	F	F	F F T	T	F
F	T	T	T T T	T	T
F	T	F	T F F	T	T
F	F	T	T T T	T	T
F	F	F	T T T	T	T

Table 12: The truth table for reasoning by transitivity.

PRINCIPLE OF CONTRAPOSITION. The statements $p \Rightarrow q$ and $\neg q \Rightarrow \neg p$ are equivalent, and so a proof of one is a proof of the other.

We have seen a truth table that shows the equivalence of the two statements earlier, in Section 8. Let us look at an example.

CLAIM. If n is a positive integer with $n^2 > 25$ then $n > 5$.

PROOF. The statement p is that n is a positive integer whose square is larger than 25. The statement q is that n is larger than 5. We could argue directly but then we would need to know something about talking square roots. Instead, let us argue indirectly. Suppose $\neg q$, that is, $n \leq 5$. By monotonicity of multiplication, we have

$$n^2 \;\leq\; 5n \;\leq\; 5 \cdot 5 \;\leq\; 25.$$

Now, by transitivity of the smaller-than-or-equal-to relation, we have $n^2 \leq 25$. Thus $\neg q$ implies $\neg p$. □

Example: Chinese remainders. Another instructive example is a result we have seen in Section 6. Let m and n be relative prime, positive integers. We map each integer in $\mathbb{Z}_{mn}$ to the pair of remainders, that is, for $0 \leq x < mn$ we define $f(x) = (x \bmod m, x \bmod n)$.

CHINESE REMAINDER THEOREM. If $x \neq y$ both belong to $\mathbb{Z}_{mn}$ then $f(x) \neq f(y)$.

PROOF. We use again the indirect approach by contraposition. Assume $f(x) = f(y)$. Then

$$\begin{aligned} x \bmod m &= y \bmod m; \\ x \bmod n &= y \bmod n. \end{aligned}$$

Hence,

$$\begin{aligned}(x-y) \bmod m &= 0;\\ (x-y) \bmod n &= 0.\end{aligned}$$

Therefore, $x-y$ is a multiple of both m and n. Hence, $(x-y) \bmod mn = 0$ and therefore $x \bmod mn = y \bmod mn$, which contradicts that $x \neq y$ in $\mathbb{Z}_{mn}$. □

Reduction to Absurdity. Another powerful indirect proof technique is by contradiction.

PRINCIPLE OF REDUCTION TO ABSURDITY. If from assuming p and $\neg q$ we can derive r as well as $\neg r$ then $p \Rightarrow q$.

Here r can be any statement. Often we use a statement r that is always true (or always false) so that we only need to derive $\neg r$ (or r) from p and $\neg q$. Let us take a look at Table 13. As with all the proof methods, it is best to see examples. There are many and a large variety because different principles are combined, or made more complicated, etc.

p	q	r	$((p \wedge \neg q) \Rightarrow (r \wedge \neg r))$	$\Rightarrow$	$(p \Rightarrow q)$
T	T	T	F T F	T	T
T	T	F	F T F	T	T
T	F	T	T F F	T	F
T	F	F	T F F	T	F
F	T	T	F T F	T	T
F	T	F	F T F	T	T
F	F	T	F T F	T	T
F	F	F	F T F	T	T

Table 13: The truth table for the reduction to absurdity.

Example: irrational numbers. A real number u is *rational* if there are integers m and n such that $u = \frac{m}{n}$ and *irrational* otherwise. The set of rational numbers is denoted as $\mathbb{Q}$. For any two different rational numbers, $u < w$, we can always find a third that lies strictly between them. For example, if $w = \frac{k}{l}$ then

$$\begin{aligned}v &= \frac{u+w}{2}\\ &= \frac{ml+nk}{nl}\end{aligned}$$

lies halfway between u and w. This property is sometimes expressed by saying the rational numbers are *dense* in the set of real numbers. How do we know that not all real numbers are rational?

CLAIM. $\sqrt{5}$ is irrational.

PROOF. Assume the square root of 5 is rational, that is, there exist integers m and n such that $\sqrt{5} = \frac{m}{n}$. Squaring the two sides, we get

$$5 = \frac{m^2}{n^2}$$

or, equivalently, $5n^2 = m^2$. But m^2 has an even number of prime factors, namely each factor twice, while $5n^2$ has an odd number of prime factors, namely 5 together with an even number of prime factors for n^2. Hence, $5n^2 = m^2$ is not possible, a contradiction. □

We take a look at the logic structure of this proof. Let p be the statement that $\sqrt{5}^2 = 5$ and q the statement that $\sqrt{5}$ is irrational. Thus $\neg q$ is the statement that $\sqrt{5} = \frac{m}{n}$. From assuming p and $\neg q$, we derive r, that is the statement $5n^2 = m^2$. But we also have $\neg r$, because each integer has a unique decomposition into prime factors. We thus derived r and $\neg r$. But this cannot be true. Using the Principle of Reduction to Absurdity, we conclude that p implies q. By modus ponens, assuming p gives q.

Summary. We have learned that theorems are tautologies and there are different ways to prove them. As applications of logic rules we have discussed direct methods (Principle of Modus Ponens) and indirect methods (Principle of Contrapositive and Principle of Reduction to Absurdity).