Languages and Computation (COMP 2049) Lab 01

Proof Techniques & Basic Concepts

(1) Use proof by contradiction to answer the following:

(a) Prove that $\sqrt{3}$ is irrational.

Solution

The proof may be carried out similar to the proof of irrationality of $\sqrt{2}$. To derive a contradiction, assume that $\sqrt{3}$ is rational. Therefore, there must exist two integers $p, q \in \mathbb{Z}$, such that:

- $q \neq 0$;
- p and q are relatively prime, i. e., they do not have a common divisor. We write this as $(p, q) = 1$;
- $\sqrt{3} = p/q$.

Therefore, $p^2 = 3q^2$, which implies that p^2 is divisible by 3. Therefore, p itself is divisible by 3 (see Claim below), i. e., $p = 3p'$ for some $p' \in \mathbb{N}$. In turn, we obtain:

$$p^2 = 3q^2 \Longrightarrow (3p')^2 = 3q^2 \Longrightarrow 3(p')^2 = q^2$$

which again implies that q also must be divisible by 3. Therefore, 3 is a common divisor of both p and q. This contradicts the assumption that p and q are relatively prime.

Claim: If the square of a natural number p is divisible by 3, then the number p must also be divisible by 3.

Proof of the Claim: Consider the natural number p, and let r denote the remainder of division of p by 3. We write this as:

$$p = r \mod (3)$$

There are three possibilities:

$\boldsymbol{r = 0}$: In this case, p is clearly divisible by 3.

$\boldsymbol{r = 1}$: We may write $p = 3k + 1$, for some natural number $k \in \mathbb{N}$. Then we have:

$$p^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1 = 1 \mod (3).$$

In this case, p^2 cannot be divisible by 3.

$\boldsymbol{r = 2}$: We may write $p = 3k + 2$, for some natural number $k \in \mathbb{N}$. Then we have:

$$p^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1 = 1 \mod (3).$$

Again, p^2 cannot be divisible by 3.

(b) Using the fact that $\sqrt{2}$ is irrational, prove that the following numbers are also irrational:

(i) $\sqrt{8}$

Solution Let us assume that $\sqrt{8}$ is rational. Then, $\sqrt{8} = p/q$ for some integers p and q. But then we have: $\sqrt{8} = 2\sqrt{2} = p/q$, which implies that $\sqrt{2} = p/(2q)$, i. e., $\sqrt{2}$ is rational. This is a contradiction.

(ii) $2 - \sqrt{2}$

Solution Assume that $2 - \sqrt{2} = p/q$. Then:

$$\sqrt{2} = 2 - \frac{p}{q} = \frac{2q - p}{q}.$$

This implies that $\sqrt{2}$ is rational, which is a contradiction.

(2) True or False:

(a) The sum of every two irrational numbers is irrational.

Solution
False. Take $a = \sqrt{2}$ and $b = -\sqrt{2}$. Both are irrational, and $a + b = 0$.

(b) The product of every two irrational numbers is irrational.

Solution
False. Take $a = \sqrt{2}$ and $b = \sqrt{2}$. Both are irrational, and $ab = 2$.

(c) [Optional] For any two irrational numbers a and b, the number a^b is irrational.

Solution
False. Let us consider the number $x = \sqrt{2}^{\sqrt{2}}$ and assume that, we do not even know whether x is rational or not. Then, there are two possibilities:

x is rational: In this case, if we take $a = b = \sqrt{2}$, then $a^b = x$ is rational.

x is irrational: In this case, let $a = x$ and $b = \sqrt{2}$. We have:

$$a^b = x^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}} = \sqrt{2}^2 = 2,$$

which is a rational number.

Note: It is indeed known that $x = \sqrt{2}^{\sqrt{2}}$ is not a rational number. The proof of this claim, however, requires application of Gelfond-Schneider theorem, a result in number theory which is beyond the scope of our module. Therefore, we proved the result without the need to know whether $\sqrt{2}^{\sqrt{2}}$ is rational or not.

(3) Using mathematical induction, prove that, for any real number $r \neq 1$ and natural number n:

$$\sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r}.$$

Solution
Let $r \neq 1$ be a real number, and let $P(n)$ denote the statement that:

$$\sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r}.$$

Base case: To prove $P(0)$, note that:

$$\sum_{i=0}^{0} r^i = r^0 = 1 = \frac{1 - r}{1 - r} = \frac{1 - r^{0+1}}{1 - r}.$$

Inductive step: Assume that for some natural number $n \in \mathbb{N}$, $P(n)$ is true. Then, we have:

$$\begin{aligned}
\sum_{i=0}^{n+1} r^i &= \sum_{i=0}^{n} r^i + r^{n+1} \\
\text{(By induction hypothesis)} &= \frac{1 - r^{n+1}}{1 - r} + r^{n+1} \\
\text{(Routine computation)} &= \frac{1 - r^{n+1} + r^{n+1} - r^{n+2}}{1 - r} \\
&= \frac{1 - r^{n+2}}{1 - r} \\
&= \frac{1 - r^{(n+1)+1}}{1 - r}.
\end{aligned}$$

This proves $P(n + 1)$.

(4) Consider the grammar $G = (V, T, S, P)$, in which $V = \{S\}$, $T = \{a, b\}$, and the set of productions is given by:

$$S \rightarrow aSa \mid bSb \mid \lambda$$

(a) Write a derivation of the string $abba$.

Solution

The following is a derivation. The production rule used in each step is written in the left-hand-side:

$$\begin{aligned}
& S \\
\text{(use production } S \rightarrow aSa\text{)} \quad & \Rightarrow aSa \\
\text{(use production } S \rightarrow bSb\text{)} \quad & \Rightarrow abSba \\
\text{(use production } S \rightarrow \lambda\text{)} \quad & \Rightarrow abba.
\end{aligned}$$

(b) Experiment with, and derive a few strings generated by, the grammar G. What language is generated by the grammar? Write down a concise description of $L(G)$.

Solution

It is easy to see that $L(G) = \left\{ww^R \,\middle|\, w \in \{a, b\}^*\right\}$, i. e., strings w over the alphabet $T = \{a, b\}$ followed by their reverses w^R. For instance, by taking $w = ab$, we obtain $ww^R = abba$.