Mathematical Foundations of Computer Science
Lecture Outline
September 3, 2024

Example. Prove that if x and y are integers where $x + y$ is even, then x and y are both odd or both even.

Solution. To prove the above claim we will prove its contrapositive which is "if exactly one of x or y is even then $x + y$ is odd". Without loss of generality, for some integers k and l, let $x = 2k$ be even and $y = 2l + 1$ be odd. Then,

$$\begin{aligned} x + y &= 2k + 2l + 1 \\ &= 2(k + l) + 1 \end{aligned}$$

Since k and l are integers so is $k + l$ and $2(k + l)$ is even and hence $x + y$ is odd.

Example. Show that at least three of any 25 days chosen must fall in the same month of the year.

Solution. Assume for contradiction that the proposition "at least three of any 25 days chosen must fall in the same month of the year" is not true. This means that each month can have at most two of the 25 days chosen. Since there are 12 months, there can be at most 24 days that must have been chosen. This contradicts the premise that we chosen 25 days. In other words, by assuming that the proposition in the question is false, we have proved that (25 days are chosen) and (at most 24 days are chosen), which is clearly a contradiction.

Example. Prove that if $3n + 2$ is odd then n is odd.

Solution. We will show the above claim is true by giving a proof by contradiction. Thus assume that $3n + 2$ is odd and n is even. Since n is even, there exists an integer k such that $n = 2k$. Thus $3n + 2$ can be written as

$$3(2k) + 2 = 2(3k + 1)$$

Since k is an integer, clearly $3k+1$ is an integer. Thus $3n+2$ is even. Note that our premise is that $3n + 2$ is odd and we have shown that $3n + 2$ is even. This is a contradiction. This proves the claim.

Example. Prove that for all real numbers a and b, if the product ab is an irrational number, then either a or b, or both must be irrational.

Solution. We will prove the above claim by proving the contrapositive. That is, we will show that if both a and b are rational numbers then their product ab is a rational number. Let $a = p/q$ and $b = r/s$, where p, q, r, and s are integers and $q \neq 0$ and $s \neq 0$. The product ab can be expressed as follows.

$$ab = \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs}$$

Note that the numerator pr is an integer and so is the denominator qs. Also, since $q \neq 0$ and $s \neq 0$, the denominator $qs \neq 0$. Thus ab is a rational number.

A Brief Detour: Set Operations.

We will make a small detour to understand operations on sets. Below are some definitions.

- Let A and B be sets. The *union* of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both. As an example, if $A = \{$Ron, Bob, Kelly$\}$ and $B = \{$Tim, Ryan, Bob$\}$ then $A \cup B = \{$Ron, Bob, Kelly, Tim, Ryan$\}$.

- Let A and B be sets. The *intersection* of the sets A and B, denoted by $A \cap B$, is the set that contains those elements that are in both A and B. For example, if $A = \{$Ron, Bob, Kelly$\}$ and $B = \{$Tim, Ryan, Bob$\}$ then $A \cap B = \{$Bob$\}$.

- Two sets are called *disjoint* if their intersection is an empty set.

- A collection of nonempty sets $\{A_1, A_2, \ldots, A_n\}$ is a *partition* of a set A if, and only if, (i) $A = \bigcup_{i=1}^{n} A_i$ and (ii) $A_1, A_2, \ldots, A_n$ are mutually (pairwise) disjoint.

- Let A and B be two sets. The *difference* of A and B, denoted by $A \setminus B$ (or $A - B$) is the set containing those elements that are in A but not in B. For example, if $A = \{1, 2, 3, 4\}$ and $B = \{2, 3, 4, 6, 8\}$ then $A \setminus B = \{1\}$.

- The *complement* of a set A is the set of elements not in A. It is denoted by $\overline{A}$. Thus, if U is the universe of elements in consideration, then the complement of set A is given by

  $$\overline{A} = U \setminus A$$

  As an example, if $U = \mathbb{N}$ and A is the set of non-negative even integers, then $\overline{A}$ is the set of all positive odd integers.

- Let A and B be sets. The *cartesian product* of A and B, denoted by $A \times B$, is the set of all ordered pairs formed by taking an element from A together with an element from B in all possible ways. That is, $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Example. Let $A = \{2^1, 2^2, 2^3, \ldots\}$ and $B = \{2, 4, 6, \ldots\}$. Prove that $A \subseteq B$.

Solution. Let x be an arbitrary but particular element in A. Element x is of the form 2^j, for some positive integer j. Note that an element in B is of the form $2 \cdot i$, for some $i \in \{1, 2, 3, \ldots\}$. Clearly, $x = 2^j = 2 \cdot i$, where $i = 2^{j-1}$. Since j is positive, $j - 1 \geq 0$ and hence $i \geq 1$. Thus $x \in B$ and hence we conclude that $A \subseteq B$.

Example. Let A and B be sets. Then, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Solution. ($\Rightarrow$): If $A = B$ then since every set is a subset of itself, we have $A \subseteq B$ and $B \subseteq A$.
($\Leftarrow$): Let x be any element in A. Since $A \subseteq B$, x is also an element in B. Similarly, if an element $y \in B$, since $B \subseteq A$, y is also an element in A. Thus there is no element in A that is not in B and there is no element in B that is not in A, that is, A and B have the same elements. By definition, $A = B$.

Example. Let $A = \{n \,|\, n = 2k + 5 \text{ for some } k \in \mathbb{N}\}$ and $B = \{n \,|\, n = 2j + 1 \text{ for some } j \in \mathbb{N}\}$. Is $A \subseteq B$?

Solution. Let x be any arbitrary but particular element in A. Then,

$$\begin{aligned} x &= 2k + 5, \quad \text{for some integer } k. \\ &= 2(k + 2) + 1 \end{aligned}$$

Since $k \in \mathbb{N}$, $k + 2 \in \mathbb{N}$, and hence we have proved that any arbitrary element $x \in A$ also belongs to the set B. Thus $A \subseteq B$.

Example. Let $A = \{n \in \mathbb{N} \,|\, n = 2k^2 - 3, \text{ for some } k \in \mathbb{N}\}$ and $B = \{n \in \mathbb{N} \,|\, n = j^2 + 3 \text{ for some } j \in \mathbb{N}\}$. Prove that $A \not\subseteq B$.

Solution. Note that $5 \in A$, since $5 = 2 \cdot 2^2 - 3$. Observe that for 5 to be an element of B, $5 = j^2 + 3$, that is, $j^2 = 2$, which is impossible since j must be a natural number. Thus we have found an element of A that does not belong to B and hence $A \not\subseteq B$.

Example. Let $A = \{n \in \mathbb{N} \,|\, n \geq 2 \text{ and } n = 4j - 5, \text{ for some } j \in \mathbb{N}\}$ and $B = \{n \in \mathbb{N} \,|\, n \geq 0 \text{ and } n = 2k + 1 \text{ for some } k \in \mathbb{N}\}$. Prove that $A \subset B$.

Solution. Let x be an arbitrary but particular element of A. We know that x is of the form $4j - 5$, where $j \in \mathbb{N}$. Thus we get

$$\begin{aligned} x &= 4j - 5 \\ &= 2 \cdot 2j - 6 + 1 \\ &= 2(2j - 3) + 1 \end{aligned}$$

Since $x \geq 2$, it must be that $4j - 5 \geq 2$. Solving for j gives us $j \geq 7/4$. Since $j \in \mathbb{N}$, we have $j \geq 2$. Thus the integer $2j - 3 \geq 1$. Thus $x \in B$ and hence $A \subseteq B$.

Note that the element $1 \in B$, but it does not belong to A. Hence $A \subset B$.

Example. Let A and B be sets. Prove that

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$$

Solution. Let $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. To prove the claim, we need to show that $X \in \mathcal{P}(A \cup B)$. Note that $X \in \mathcal{P}(A)$ or $X \in \mathcal{P}(B)$. Without loss of generality, let $X \in \mathcal{P}(A)$. Thus X is a subset of A. Since every element of A is also an element of $A \cup B$, X is also a subset of $A \cup B$. By definition, $X \in \mathcal{P}(A \cup B)$. This completes the proof.

Example. Recall the *cartesian product* of A and B, denoted by $A \times B$, is the set of all ordered pairs formed by taking an element from A together with an element from B in all possible ways. That is, $A \times B = \{(a, b) \,|\, a \in A, b \in B\}$. Prove that if A and B are non-empty sets then $A \times B = B \times A$ iff $A = B$.

Solution. First we will prove that if $A = B$ then $A \times B = B \times A$. Since $A = B$, $A \times B = A \times A = B \times A$.

Now assume that $A \times B = B \times A$. We will show that $A = B$. Let x be any arbitrary but particular element in A. Consider any element $y \in B$. Note that y must exist since $B \neq \emptyset$. Since $A \times B = B \times A$, the element (x, y) is in $A \times B$ as well as $B \times A$. Hence $x \in B$, which means $A \subseteq B$. The proof for $B \subseteq A$ is along the same lines.

Do you see why the condition that A are B are non-empty is necessary? Suppose that one of the sets is empty and the other is not. Then $A \times B = B \times A = \emptyset$, but $A \neq B$.

DeMorgan's Laws Let A, B, and C be sets. Then

$$\begin{aligned} A - (B \cup C) &= (A - B) \cap (A - C) \\ A - (B \cap C) &= (A - B) \cup (A - C) \end{aligned}$$

Example. Prove that the product of two odd numbers is an odd number.

Solution. Let x and y be particular but arbitrarily chosen odd numbers. Then, $x = 2k+1$ and $y = 2l + 1$, for some integers k and l. We have

$$x \cdot y = (2k + 1) \cdot (2l + 1) = 4kl + 2(k + l) + 1 = 2(2kl + k + l) + 1$$

Let $p = 2kl + k + l$. Since k and l are integers, p is an integer and $x \cdot y = 2p + 1$ is odd.

Example. Prove that $\sqrt{2}$ is irrational.

Solution. For the purpose of contradiction, assume that $\sqrt{2}$ is a rational number. Then there are integers a and b ($b \neq 0$) with no common factors such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of the above equation gives

$$\begin{aligned} 2 &= \frac{a^2}{b^2} \\ a^2 &= 2b^2 \qquad (1) \end{aligned}$$

From (1) we conclude that a^2 is even. This fact combined with the result of previous example implies that a is even. Then, for some integer k, let

$$a = 2k \qquad (2)$$

Combining (1) and (2) we get

$$\begin{aligned} 4k^2 &= 2b^2 \\ 2k^2 &= b^2 \end{aligned}$$

The above equation implies that b^2 is even and hence b is even. Since we know a is even this means that a and b have 2 as a common factor which contradicts the assumption that a and b have no common factors.

We will now give a very elegant proof for the fact that "$\sqrt{2}$ is irrational" using the *unique factorization theorem* which is also called the *fundamental theorem of arithmetic.*

The unique factorization theorem states that every positive number can be uniquely represented as a product of primes. More formally, it can be stated as follows.

> Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that
>
> $$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}$$
>
> and any other expression of n as a product of primes is identical to this except, perhaps, for the order in which the factors are written.