Mathematical Induction

Principle of Mathematical Induction

- An example of inductive proof:

  Show that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ is true for all $n \in \mathbf{Z}^+$.

  The inductive proof consists of two parts.

  First, we show that the statement is true for the base case, i.e., for $n = 1$.

  Second, we assume that the statement is true for n, and then show that it is also true for $n + 1$.

- Does $\mathbf{Z}^+$ have any distinct property against $\mathbf{Q}^+$ and $\mathbf{R}^+$?

$$\mathbf{Z}^+ = \{x \in \mathbf{Z} \mid x > 0\} = \{x \in \mathbf{Z} \mid x \geq 1\}$$

$$\mathbf{Q}^+ = \{x \in \mathbf{Q} \mid x > 0\}, \qquad \mathbf{R}^+ = \{x \in \mathbf{R} \mid x > 0\}$$

- The well-ordering principle:

  Every nonempty subset of $\mathbf{N}$ contains a smallest element

  ($\mathbf{N}$ is well-ordered)

  - Can be used to prove the principle of mathematical induction
  - $\mathbf{R}^+$ is not well-ordered

- Theorem: The Principle of Mathematical Induction

  Let $P(n)$ be a proposition for a natural number n.

  - If $P(0)$ is true; and
  - If $(\forall k \in \mathbf{N})\ (P(k) \rightarrow P(k+1))$ is true;

  Then, $(\forall n \in \mathbf{N})\ P(n)$ is true

- Consider applying the Modus Ponens

$$
\begin{array}{ll}
P(0) & \\
P(0) \rightarrow P(1) & P(1) \\
P(1) \rightarrow P(2) & P(2) \\
\quad \cdots\cdots & \quad \cdots \\
P(k) \rightarrow P(k+1) & P(k+1)
\end{array}
$$

Proof (by contradiction):

Suppose $(\forall n \in \mathbf{N})\ P(n)$ is not true.

If we let $F = \{t \in \mathbf{N} \mid P(t) \text{ is false}\}$, $F \neq \varnothing$.

Then, there must be a smallest element $s \in F$ by the well-ordering principle. Notice that $P(s)$ is false.

Since $P(0)$ is true, $s \neq 0$.

So, $s > 0$ and thus $s - 1 \in \mathbf{N}$.

With $s - 1 \notin F$ we have $P(s - 1)$ true.

Therefore, $P((s - 1) + 1) = P(s)$ is true, which is a contradiction.

Examples

- For all $n \in \mathbf{Z}^{+}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Proof:

(Basis step) For $n = 1$

LHS = 1, RHS = 1. So, LHS = RHS.

(Inductive step)

We want to show that

$$(\forall n \in \mathbf{N}) \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \Rightarrow \quad \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$$

Proof:

Let $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ (Additional premise, or Inductive Hypothesis)

Then,

$$\sum_{i=1}^{n+1} i = (n+1) + \sum_{i=1}^{n} i$$

$$= (n+1) + \frac{n(n+1)}{2}$$ (by the inductive hypothesis)

$$= \frac{2(n+1) + n(n+1)}{2}$$

$$= \frac{(n+1)(n+2)}{2}$$

Proof:

By applying the CP rule, we get

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \Rightarrow \quad \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$$

Since our choice of n for the inductive hypothesis was arbitrary,

$$(\forall n \in \mathbf{N}) \quad \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad \Rightarrow \quad \sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2} \qquad \text{(UG)}$$

- Let $r \neq 0$ and $r \neq 1$

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

Proof:

(Basis step) For $n = 0$

LHS = 1, RHS = 1. So, LHS = RHS.

(Inductive step)

Let $\sum_{i=0}^{n} r^i = \dfrac{r^{n+1} - 1}{r - 1}$ (AP, i.e., Inductive Hypothesis)

Proof:

We want to show that $\sum_{i=0}^{n+1} r^i = \frac{r^{n+2}-1}{r-1}$

(and we will apply the CP rule)

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

$$= r^{n+1} + \frac{r^{n+1}-1}{r-1}$$ (by the Inductive Hypothesis)

$$= \frac{r^{n+2} - r^{n+1} + r^{n+1} - 1}{r-1} = \frac{r^{n+2}-1}{r-1}$$

- For all $n \in \mathbf{Z}^+$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

Proof:

(Basis step) For $n = 1$

LHS = 1, RHS = 1. So, LHS = RHS.

(Inductive step)

Let $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$ (Inductive Hypothesis)

We want to show that $\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2n+3)}{6}$

Proof:

$$\sum_{i=1}^{n+1} i^2 = (n+1)^2 + \sum_{i=1}^{n} i^2$$

$$= (n+1)^2 + \frac{n(n+1)(2n+1)}{6}$$ (by the Inductive Hypothesis)

$$= \frac{6(n+1)^2 + n(n+1)(2n+1)}{6} = \frac{(n+1)[6(n+1) + n(2n+1)]}{6}$$

$$= \frac{(n+1)(2n^2 + 7n + 6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

- For every $n \in \mathbf{N}$, $7^n - 2^n$ is divisible by 5.

Proof:

(Basis step) For $n = 0$

$7^0 - 2^0 = 0$ is divisible by 5.

(Inductive step)

Let $7^n - 2^n$ be divisible by 5.

Then,

$$7^{n+1} - 2^{n+1} = 7\cdot(7^n - 2^n) + 7\cdot 2^n - 2^{n+1}$$

$$= 7\cdot(7^n - 2^n) + 2^n\cdot(7 - 2)$$

Proof:

Since $(7^n - 2^n)$ is divisible by 5 by the inductive hypothesis, $7 \cdot (7^n - 2^n)$ is divisible by 5.

Also, $2^n \cdot (7 - 2)$ is divisible by 5.

Therefore, $7^{n+1} - 2^{n+1}$ is divisible by 5.

- If S is a finite set then $|\wp(S)| = 2^{|S|}$.

Proof:

(Basis step) For $S = \varnothing$

LHS $= |\wp(\varnothing)| = |\{\varnothing\}| = 1 = 2^0 = 2^{|\varnothing|} =$ RHS.

(Inductive step)

Let $|\wp(S)| = 2^{|S|} = 2^n$ for $S = \{a_1, a_2, \ldots, a_n\}$.

We want to prove that $|\wp(S')| = 2^{|S'|} = 2^{n+1}$

where $S' = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$.

Proof:

We know that if $X \subseteq S$ then $X \subseteq S'$, which means that every subset of S is a subset of S'.

But, note that $X \cup \{a_{n+1}\} \subseteq S'$ for any $X \subseteq S$ and there is no other subset of S' in addition to these subsets.

Therefore, the number of subsets of S' is twice that of S, i.e.,

$$|\wp(S')| = 2 \cdot |\wp(S)| = 2 \cdot 2^{|S|} = 2 \cdot 2^{n} = 2^{n+1} = 2^{|S'|}.$$

- The number of left parenthesis is equal to the number of right parenthesis in a propositional well-formed formula.

Proof:

Let $\#L(\mathbf{F})$ and $\#R(\mathbf{F})$ denote the number of left parenthesis and the number of right parenthesis of a wff $\mathbf{F}$, respectively.

(Basis Step)

Since any propositional variable or constant S has no parenthesis by the basis clause of the inductive definition of a wff, $\#L(S) = \#R(S)$.

Proof:

(Inductive Step)

Let P and Q be two wffs such that

$$\#L(P) = \#R(P) \text{ and } \#L(Q) = \#R(Q).$$

Let $\mathbf{F}$ be any one of the formulas defined by the inductive clause of the inductive definition of a wff, that is, $(\neg P)$, $(P \vee Q)$, $(P \wedge Q)$, $(P \to Q)$, and $(P \leftrightarrow Q)$.

If $\mathbf{F} = (\neg P)$, then $\#L(\mathbf{F}) = \#L(P) + 1$ and $\#R(\mathbf{F}) = \#R(P) + 1$.

Therefore, $\#L(\mathbf{F}) = \#R(\mathbf{F})$.

Proof:

On the other hand, if $\mathbf{F}$ is $(P \vee Q)$, $(P \wedge Q)$, $(P \rightarrow Q)$, or $(P \leftrightarrow Q)$, then

$\#L(\mathbf{F}) = \#L(P) + \#L(Q) + 1$ and

$\#R(\mathbf{F}) = \#R(P) + \#R(Q) + 1$.

Again, since $\#L(P) = \#R(P)$ and $\#L(Q) = \#R(Q)$,

$\#L(\mathbf{F}) = \#R(\mathbf{F})$.