What is the mathematical induction?

October 27, 2012

Suppose we have to prove the following sentence $\forall_{n\in\mathbf{N}}\ T(n)$, where T stands for *propositional form*. In mathematics, the example of such a construction can be an *equality*. Let us consider the following equality

$$1+2+\ldots+n=\frac{1+n}{2}\cdot n. \tag{1}$$

We note, that in this form, (1) is not a *logical sentence*. If in (1), we treat n as *variable*, then we obtain the propositional form T with the *origin* $\mathbf{N}$, where

$$T(n):\quad 1+2+\ldots+n=\frac{1+n}{2}\cdot n,\ n\in\mathbf{N}. \tag{2}$$

Now, by using the standard construction $\forall_{n\in\mathbf{N}}\ T(n)$ we get the logical sentence and we can try to prove the truth of the sentence. One of the effective methods to realize such a proof is *the Principle of Mathematical Induction* (PMI).

PMI is the mathematical theorem which consists of two steps: *the initialing step* and *the induction step*. The first step is reduced to check the condition: whether the statement $T(1)$ is true. The induction step requires to verifying the implication

$$\forall_{k\geq 1}\ (T(k)\rightarrow T(k+1)). \tag{3}$$

The PIM says, that if both steps are fulfilled, then $\forall_{n\in\mathbf{N}}\ T(n)$.

In the case of (2) $T(1)$ is true. To see that the induction step is satisfied, we suppose that for given $k\geq 1$, the sentence

$$T(k):\quad 1+2+\ldots+k=\frac{1+k}{2}\cdot k \tag{4}$$

is true. According to PMI, all what we nedd to do is to show that the sentence $T(k+1)$ is true as well. By assumption (4) we get

$$1+2+\ldots+k+k+1=\frac{1+k}{2}\cdot k+k+1=(k+1)(\frac{k}{2}+1)=\frac{1+k+1}{2}\cdot(k+1),$$

which means that the condition (3) is true. Therefore, by a PMI the sentence $\forall_{n\in\mathbf{N}}\ T(n)$ is true.

Now we use the PMI to prove the following theorem

Theorem 1 *Let X be a finite set with cardinality n, so $|X|=n$. Then the cardinality of the family $\mathcal{P}(X)$ consists of all subset of X is equal to 2^n. Therefore, we can write*

$$|\mathcal{P}(X)|=2^{|X|}.$$

Proof. Let us consider the propositional form $T(n)$ as the equality $|\mathcal{P}(X)| = 2^n$, for $n \geq 1$. If $n = 1$, then $|X| = 1$ and $\mathcal{P}(X) = \{\emptyset, X\}$, hence the sentense $T(1)$ is true. Assume that for $k \geq 1$, $|X| = k$ implies $|\mathcal{P}(X)| = 2^k$, i.e., the sentence $T(k)$ is true. All we need is to prove that the sentence $T(k+1)$ also is true. If $|X| = k+1$ we can assume that $X = Y \cup \{a\}$, where $|Y| = k$, for some element $a \notin Y$. Now for family of all subsets of X we have

$$\mathcal{P}(X) = \mathcal{P}(Y) \cup \mathcal{P}_a(Y),$$

where in the above union the last family $\mathcal{P}_a(Y)$, consists of all subset A of X of the form $A = B \cup \{a\}$ for certain sets $B \subset Y$. Indeed, if we take any subset A of X then we have two cases: $a \notin A$ or $a \in A$. In the first, this means that $A \subset Y$ and consequently $A \in \mathcal{P}(Y)$. Otherwise, $A = B \cup \{a\}$ for $B \subset Y$, therefore $A \in \mathcal{P}_a(Y)$, by definition of the family $\mathcal{P}_a(Y)$. Since those both families are pairwise disjoint, by *additivity rule* we have

$$|\mathcal{P}(X)| = |\mathcal{P}(Y)| + |\mathcal{P}_a(Y)|.$$

Now it is suffices to observe, that because of the correspondence

$$B \longrightarrow A \cup \{a\},$$

which is a *bijection*, the families $\mathcal{P}(Y)$ and $\mathcal{P}_a(Y)$ are the same number. Hence $|\mathcal{P}(Y)| = |\mathcal{P}_a(Y)|$. But by the induction assumption, $|\mathcal{P}(Y)| = 2^k$, which completes the proof.

□

Remark 1 *The number 2^n as well known, is fundamental in computer science–it is the cardinality of the set of all binary sequences of the length n. Therefore, if $\mathbf{B(n)}$ denotes such a set, then $|\mathbf{B(n)}| = |\mathcal{P}(X)|$, where $|X| = n$. It is implies the existence of the bijection $f\colon \mathcal{P}(X) \to \mathbf{B(n)}$. Below we give a costruction of such bijection.*

Example 1 *For the fixed natural n, let $X = \{x_1, x_2, \ldots, x_n\}$. Further we need any arrangement of the set X. Without loss of generality, we assume that this arrangement is represented by the above definition of the set X. Now, for every non empty subset A of X, if we order the elements of A in accordance with X, then the set A can be coded by the binary sequence $(b_1, b_2, \ldots, b_n)$, where $b_j = 1$ iff in the set A there exists an element x_j, otherwise $b_j = 0$. It is easy to see that such defined correspondence $A \to (b_1, b_2, \ldots, b_n)$ is one–to–one and on, so it is a bijection if in addition, by definition we assume that the sequence $(0, 0, \ldots, 0)$ corresponds to empty set.*

Remark 2 *On the other hand, the set $\mathbf{B(n)}$ represents the set of all functions defined on the n–th elements set with values in the 2–elements set. From the combinatorics is well known, that for this reason, the cardinality of the $\mathbf{B(n)}$ is equal to 2^n. This gives us another proof of the theorem 1.*