1.4.5 Principle of mathematical induction – continuation

Example. Derive a formula for $\sum_{i=0}^{n} i^2$ and prove it.

Solution. Our guess will be that it as some polynomial of degree 3. (It is a generalization of the fact the $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.) A general polynomial of degree 3 is $an^3 + bn^2 + cn + d$.

If $\sum_{i=0}^{n} i^2 = an^3 + bn^2 + cn + d$ is a correct formula then it has to be valid for any $n \geq 0$. If we would like to prove the formula using mathematical induction we should have to show that the unknown coefficients a, b, c, d satisfy the basic and the inductive step.

Let us first examine the basic step:
For $n = 0$, it must hold

$$0 = \sum_{i=0}^{0} i^2 = a \cdot 0^3 + b \cdot 0^2 + c \cdot 0 + d = d.$$

Hence $d = 0$ and if the formula will be correct then $\sum_{i=0}^{n} i^2 = an^3 + bn^2 + cn$.

Now, let us deal with the inductive step. Assume that $\sum_{i=0}^{n} i^2 = an^3 + bn^2 + cn$. We have to show that $\sum_{i=0}^{n+1} i^2 = a(n+1)^3 + b(n+1)^2 + c(n+1)$. We know that

$$\sum_{i=0}^{n+1} i^2 = \sum_{i=0}^{n} i^2 + (n+1)^2.$$

Hence the coefficients a, b, c have to satisfy

$$a(n+1)^3 + b(n+1)^2 + c(n+1) = an^3 + bn^2 + cn + (n+1)^2.$$

Two polynomials are equal if, and only if the corresponding coefficients are equal. We get the following system of linear equations

$$\begin{array}{ccccccc} 3a & & & & & = & 1 \\ 3a & + & 2b & & & = & 2 \\ a & + & b & + & c & = & 1 \end{array}$$

The only solution of the system above is $a = \frac{1}{3}$, $b = \frac{1}{2}$, and $c = \frac{1}{6}$. Therefore,

$$\sum_{i=0}^{n} i^2 = \frac{1}{3} n^3 + \frac{1}{2} n^2 + \frac{1}{6} n = \frac{n(2n+1)(n+1)}{6}.$$

1.4.6 Theorem. The principle of mathematical induction follows from the well-ordering principle.

Proof. Assume that for a property $V(n)$ there is $n_0 \in \mathbb{N}$ such that the following conditions hold:

1. $V(n_0)$ is true.
2. If $V(n)$ is true for a natural number $n \geq n_0$ then so is $V(n+1)$.

Denote by M the set of all natural numbers $n \geq n_0$ for which $V(n)$ is not true. Assume that M has the smallest element, say n_1. Clearly, $n_1 \neq n_0$ because $V(n_0)$ is true. Hence, $n_1 > n_0$. Take $n_2 = n_1 - 1$; then $n_2 \geq n_0$. Since n_1 is the smallest element of M, $n_2 \notin M$, which means that $V(n_2)$ is true. But then by the condition 2), $V(n_1)$ it true as well, indeed, $n_1 = n_2 + 1$. A contradiction.

Therefore, M does not have smallest element which, by well-ordering principle, means that $M = \emptyset$. We have shown that $V(n)$ is true for all natural numbers $n \geq n_0$, which is what principle of mathematical induction claims.

1.4.7 Remark. The principle of weak mathematical induction is not always sufficient when e.g. proving some facts. Here, we introduce a new version of mathematical induction, called a strong mathematical induction, which is equivalent to the weak one but helps to solve situations where the weak one does not suffice.

1.4.8 Principle of Strong Mathematical Induction. Given a property $V(n)$ that may be true or false for $n \in \mathbb{N}$. Let n_0 be a natural number. Assume that the following conditions hold:

1. $V(n_0)$ holds.
2. If $V(k)$ holds for every natural number k, $n_0 \leq k < n$, then so does $V(n)$.

Then $V(n)$ holds for all natural numbers $n \geq n_0$.

Notice, that the principle of strong mathematical induction differs from the weak one in the second condition. In the weak induction we assume that $V(n-1)$ is true and from it we deduce that $V(n)$ is true as well. In the strong version, the induction assumption is that $V(k)$ holds for **every** k, $n_0 \leq k < n$. From this assumption we show that $V(n)$ is true as well.

1.4.9 Example. Let us prove by strong mathematical induction the following statement: *Every natural number $n \geq 2$ is a product of one or more primes.*

Recall that: A prime number is a natural number $p > 1$ such that if $p = r \cdot s$ for natural numbers r, s then either $r = 1$ or $s = 1$. A natural number $n > 1$ which is not a prime is called a composite number.

Solution: We proceed by strong mathematical induction.

Basic step. The number $n = 2$ is a prime number. So the statement is true for $n = 2$.

Inductive step. Assume that all natural numbers k such that $2 \leq k < n$ are products of one or more primes. Consider the number n. Then either n is a prime number of n is a composite number. If n is a prime then it is a product of one prime number.

Assume that n is a composite number. Then $n = r \cdot s$ where $1 < r, s < n$. From the induction assumption, we know that r and s are products of one or more primes, hence n is a product of primes as well.

1.4.10 Theorem. The weak and the strong mathematical induction are equivalent.

Justification. It is not difficult to see that whenever a property $V(n)$ satisfies 2w) and $V(n)$ is true, then $V(k)$ is true for every k, $n_0 \leq k \leq n$. Indeed, assume that there is k, $n_0 \leq k \leq n$. Take the smallest one and denote it by k_0. Then $k_0 > n_0$, since $V(n_0)$ is true by the condition 1). Consider $k_0 - 1 \geq n_0$; because k_0 is the smallest one for which $V(k)$ is not true, $V(k_0 - 1)$ is true. But in this case, the condition $V(k_0)$ must be true, this follows from the condition 2w). A contradiction.

1.4.11 Theorem. The well-ordering principle follows from the strong version of mathematical induction.

Proof. Assume that the strong version of mathematical induction holds. Let M be a set of natural numbers that does not have the smallest element. We shall show that M is empty.

Consider the property $V(n)$ defined by

$$V(n) \text{ is true if, and only if } n \notin M.$$

The property $V(n)$ satisfies 1) for $n_0 = 0$, and 2s). Indeed:

1. Basic step. $V(0)$ is true. Indeed, if $0 \in M$ then 0 is the smallest element of M, which contradicts to the fact that M does not have the smallest element.

2s. Inductive step. Assume that for all $k \leq n$ it holds $k \notin M$ ($V(k)$ is true). Then $n+1$ cannot be in M, indeed it would have been the smallest element of M. Hence, $V(n+1)$ is true.

By strong mathematical induction, $V(n)$ is true for all $n \in \mathbb{N}$, which means that no natural number belongs to M; therefore M is empty.

1.4.12 Tiling Problem. A right tromino is a figure consisting in three squares of the same size arranged to a right angle. A deficient board of 2^{2n} squares is a square with one square missing.

Is it possible to cover a deficient boar by trominos for every $n \geq 1$.

The fact that the answer is yes, can be proved by induction.

Basic step. For $n = 1$ a deficient board of 2^2 squares is just one tromino.

Inductive step. Assume that any deficient board of 2^{2n} squares can be covered by trominos. Consider a deficient board of $2^{2(n+1)}$ squares. Divide the board into 4 boards of 2^{2n} squares, one of which is a deficient board. Place one tromino in the center so that now all 4 boards are deficient. Since now all the 4 boards are deficient, we can use the induction assumption to cover it by trominos.

1.4.13 Hanoi Towers. Three pegs A, B, C are given together with n discs of different size. All discs are placed to peg A. The task is to move all n discs to peg B or C. The rule for moving a disc is the following: A disc can be placed only on a bigger one.

Compute the smallest number of moves that are needed to move n discs from peg A to peg B.

To move the biggest disc (which is the bottom one on peg A) one must first move all $n-1$ smaller discs to one of the pegs B or C, then the biggest one must be moved to an empty peg. Finally, all the $n-1$ smaller ones must move on the biggest one.

Hence the following formula for the number of moves $T(n)$ holds:

$$T(n) = 2 \cdot T(n-1) + 1, \quad T(1) = 1.$$

It is not difficult to guess and afterwards prove that

$$T(n) - \sum_{i=0}^{n} 2^{n-1} = 2^n - 1.$$

1.4.14 Structural Induction. Mathematical induction is used not only to prove some statement but also to define a set. Let us start with an example.

Example. The set B of all binary words can be defined as follows:

Basic step. The empty word belong to B, i.e. $\varepsilon \in B$.

Inductive step. If $w \in B$ then $w0 \in B$ and $w1 \in B$.

The basic step lists "small" elements of the set. The inductive step tells how to get "more complex" elements from those that were already formed.

1.4.15 Let A be a set of binary words defined inductively by:

- $0 \in A$ and $1 \in A$.
- If $w \in A$ then $0w0 \in A$ and $1w1 \in A$.

Prove that A consists of all binary words of odd length which are palindromes (i.e. words w that are the same as its reverse).

Solution. Denote by A' the set of all binary words that are palindromes. We have to show that $A = A'$.

First, let us prove that $A \subseteq A'$, in other words, that every word $w \in A$ is a palindrome of odd length. We proceed as follows:

1. 0 and 1 are palindromes of odd length.
2. If w is a palindrome of odd length then so are $0w0$ and $1w1$.

Since all elements from A were constructed using finite number of steps 1. and 2., we proved that every element of A belongs to A'.

Now, let us prove that $A' \subseteq A$; in other words, that every odd palindrome can be obtained by the procedure above. We shall proceed by induction on the length $2n - 1$ of w.

Basic step. For $n = 1$ there are only two palindromes of length 1; indeed, they are 0 and 1. Both belong to A.

Inductive step. Assume that any palindrome of length $2n - 1$ can be formed by tho rules 1) and 2) (i.e. they belong to A). Take any palindrome w of length $2n + 1$, and denote by a its first bit. Then a is either 0 or 1. Since w is a palindrome, the first bit must be the same as the last one. Hence, $w = aua$ for a palindrome u of length $2n - 1$. Therefore, $u \in A$, which proves that $aua \in A$ as well.

Hence, by the mathematical induction we get that $A = A'$; in other words, A consists of all palindromes of odd length.

The first part of the proof is called *structural induction.*