Discrete Mathematics

Session XII

Induction and Inductive Definitions

Mehran S. Fallah

June 2020

Introduction

Having known about the integers since our first encounters with arithmetic, we examine a special property exhibited by the subset of ***positive integers***.

This property will enable us to establish certain mathematical formulas and theorems by using a technique called ***mathematical induction***.

This method of proof will play a key role in many of the results you have already seen as well those you may encounter in the future.

In this session, we introduce the so-called ***well-ordering principle***, a property of the set of positive integers.

Then, we introduce the principle of mathematical induction. It is also explained how it leads to a useful ***proof principle***.

We state two versions of this proof principle, the ***weak*** and the ***strong*** forms of induction on positive integers.

The principle is then generalized so that it can be employed in the proof of statements on the sets other than positive integers.

Well-Ordering and Mathematical Induction

The well-ordering principle: The set $\mathbb{Z}^+$ of positive integers is well ordered by the ordinary partial order relation $\leq$. That is, every nonempty subset of $\mathbb{Z}^+$ has a least (smallest) element. More formally,

$$\forall X \subseteq \mathbb{Z}^+.(X \neq \emptyset \longrightarrow \exists a \in X.\forall x \in X.a \leq x).$$

The principle of mathematical induction: Let A be a subset of $\mathbb{Z}^+$ such that

1) $1 \in A$, and
2) for every $k \in \mathbb{Z}^+$, if $k \in A$ then $k + 1 \in A$.

Then, $A = \mathbb{Z}^+$.

Both the principles are ***intuitive*** (each of them can be taken as an ***axiom***, which everyone accepts without any proof.)

However, one logically implies the other.

The well-ordering principle $\Longrightarrow$ The principle of mathematical induction

The principle of mathematical induction $\Longrightarrow$ The well−ordering principle

If we take the well-ordering principle as an axiom, the principle of mathematical induction will be a theorem.

If we take the principle of mathematical induction as an axiom, the well-ordering principle will be a theorem.

Mathematical Induction

Theorem 1. Let A be a subset of $\mathbb{Z}^+$ such that

1) $1 \in A$, and
2) for every $k \in \mathbb{Z}^+$, if $k \in A$ then $k + 1 \in A$.

Then, $A = \mathbb{Z}^+$.

Proof. Assume that A is a subset of $\mathbb{Z}^+$ that satisfies (1) and (2). Assume also that $A \neq \mathbb{Z}^+$ (proof by contradiction.) Because $A \subseteq \mathbb{Z}^+$ and $A \neq \mathbb{Z}^+$, the set $\mathbb{Z}^+ - A$ is a nonempty subset of $\mathbb{Z}^+$. Thus, by the well-ordering principle, $\mathbb{Z}^+ - A$ has a smallest element m. As m is a positive integer and $m \neq 1$, $m - 1 \in A$ (otherwise, m could not be a smallest element of $\mathbb{Z}^+ - A$.) From (2), it follows that $(m - 1) + 1 = m \in A$. Hence, both $m \in A$ and $m \in \mathbb{Z}^+ - A$ hold, which is a contradiction.

This theorem is knows as the (***weak*** form of the) principle of mathematical induction. It can also be expressed in a first-order language as follows:

For every subset A of $\mathbb{Z}^+$,

$$\big(1 \in A \ \wedge\ \forall k \in \mathbb{Z}^+.(k \in A \longrightarrow k + 1 \in A)\big) \implies A = \mathbb{Z}^+.$$

The principle of mathematical induction can be turned into a ***proof principle***.

Mathematical Induction (Ctd.)

Corollary 1. Let α be a unary predicate on positive integers. Then,

$$\Big(\alpha(1) \wedge \forall k \in \mathbb{Z}^+.\big(\alpha(k) \longrightarrow \alpha(k+1)\big)\Big) \Longrightarrow \forall n \in \mathbb{Z}^+.\alpha(n).$$

Proof. We must prove that $\forall n \in \mathbb{Z}^+.\alpha(n)$ is true whenever the formula $\Big(\alpha(1) \wedge \forall k \in \mathbb{Z}^+.\big(\alpha(k) \longrightarrow \alpha(k+1)\big)\Big)$ is true. Let $A = \{n \in \mathbb{Z}^+ \mid \alpha(n) \text{ is true.}\}$. We have $A \subseteq \mathbb{Z}^+$. Since $\alpha(1)$ is true, $1 \in A$. Moreover, $\forall k \in \mathbb{Z}^+.\big(\alpha(k) \longrightarrow \alpha(k+1)\big)$ implies that $\forall k \in \mathbb{Z}^+.(k \in A \longrightarrow k+1 \in A)$. Thus, by the principle of mathematical induction, $A = \mathbb{Z}^+$. Consequently, $\forall n \in \mathbb{Z}^+.\alpha(n)$ is true.

This makes a proof principle. To show that a predicate α is true for all positive integers, one can equivalently show that

1) α is true for 1, and
2) for every positive integer k, if α is true for k, then it is true for $k+1$.

$$\Big(\alpha(1) \wedge \forall k \in \mathbb{Z}^+.\big(\alpha(k) \longrightarrow \alpha(k+1)\big)\Big) \Longrightarrow \forall n \in \mathbb{Z}^+.\alpha(n).$$

Induction Basis

Induction Step

Induction Hypothesis

Induction Conclusion

$\big(\alpha(1) \wedge \forall k \in \mathbb{Z}^+.\big(\alpha(k) \longrightarrow \alpha(k+1)\big)\big) \Longrightarrow \forall n \in \mathbb{Z}^+.\alpha(n).$

Mathematical Induction (Ctd.)

Example 1. Among the many interesting sequences of numbers encountered in discrete mathematics and combinatorics, one finds the ***harmonic numbers*** $H_1, H_2, H_3, \ldots$, where

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

for each $n \in \mathbb{Z}^+$. Prove that the following holds for every positive integer n.

$$\sum_{j=1}^{n} H_j = (n+1)H_n - n.$$

Solution. Let $p(n)$ be $\sum_{j=1}^{n} H_j = (n+1)H_n - n$. We must prove that $\forall n \in \mathbb{Z}^+.p(n)$. From Corollary 1, we can equivalently show that $p(1)$ is true, and, for every $k \in \mathbb{Z}^+$, if $p(k)$ is true, then so is $p(k+1)$. The statement $p(1)$ is

$$\sum_{j=1}^{1} H_j = (1+1)H_1 - 1.$$

That is, $H_1 = 2H_1 - 1$ or $1 = 2 \cdot 1 - 1$. Thus, $p(1)$ is true. For the induction step, let k be an arbitrary positive integer such that $p(k)$ is true. In other words, the induction hypothesis $\sum_{j=1}^{k} H_j = (k+1)H_k - k$ is true. We must prove that the following is true.

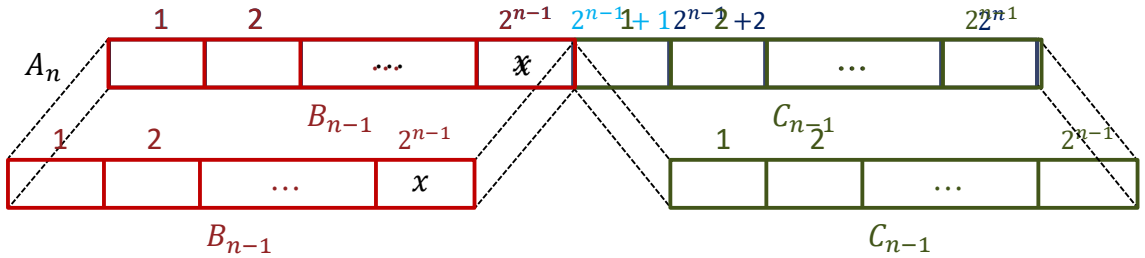
$$\sum_{j=1}^{k+1} H_j = ((k+1)+1)H_{k+1} - (k+1) = (k+2)H_{k+1} - k - 1.$$

We have

$$\sum_{j=1}^{k+1} H_j = \sum_{j=1}^{k} H_j + H_{k+1} = \big((k+1)H_k - k\big) + H_{k+1}$$

$$= (k+1)\left(H_{k+1} - \frac{1}{k+1}\right) - k + H_{k+1} = (k+2)H_{k+1} - k - 1.$$

Mathematical Induction (Ctd.)



$\alpha(n)$: For any given real number r and any 2^n-element tuple A_n that is sorted in ascending order, the procedure compares r with no more than $n + 1$ elements of the tuple.

We must show that $\alpha(1)$ is true. Assume that $A_1 = (a, b)$. We first compare r with a. If $r = a$, the procedure terminates and r is in A_1. If $r < a$, r is not in A_1. If $a < r$, we compare r with b. Thus, the procedure compare r with no more than $1 + 1 = 2$ elements of A_1. For the induction step, assume that k is an arbitrary positive integer and that $\alpha(k)$ is true. Now, let A_{k+1} be a 2^{k+1}-element tuple of real numbers. Divide A_{k+1} into the 2^k-element tuples B_k and C_k. The procedure compares r with $x = B_k[2^k]$. If $r = x$, the search terminates. If $r < x$, the procedure searches for r in B_k. Otherwise, it looks for r in C_k. From the induction hypothesis, each of the two latter cases requires no more than $k + 1$ comparisons. Thus, the procedure does not compare r with more than $1 + (k + 1) = k + 2$ elements of A_{k+1}.

Generalizations

Corollary 2. Let α be a unary predicate on the set $\mathbb{Z}^{\geq n_0} = \{n \in \mathbb{Z} \mid n \geq n_0\}$. Then,

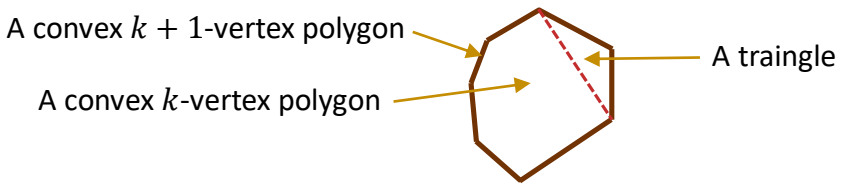
$$\Big(\alpha(n_0) \wedge \forall k \in \mathbb{Z}^{\geq n_0}.\big(\alpha(k) \longrightarrow \alpha(k+1)\big)\Big) \Longrightarrow \forall n \in \mathbb{Z}^{\geq n_0}.\alpha(n).$$

Example 3. Prove that the sum of the interior angles of a convex n-vertex polygon equals $(n-2)\cdot 180°$.

Proof. Let $\beta(n)$ be $\alpha(n+n_0-1)$, β is a predicate on positive integers. We have

$$\Big(\alpha(n_0) \wedge \forall k \in \mathbb{Z}^{\geq n_0}.\big(\alpha(k) \longrightarrow \alpha(k+1)\big)\Big)$$
$$\Leftrightarrow \Big(\beta(1) \wedge \forall k \in \mathbb{Z}^{+}.\big(\beta(k) \longrightarrow \beta(k+1)\big)\Big)$$
$$\Longrightarrow \forall n \in \mathbb{Z}^{+}.\beta(n) \Longrightarrow \forall n \in \mathbb{Z}^{+}.\alpha(n+n_0-1) \Rightarrow \forall n \in \mathbb{Z}^{\geq n_0}.\alpha(n)$$

Solution. Let $p(n)$ be "the sum of interior angles of any convex n-vertex polygon is $(n-2)\cdot 180°$." We must prove that $\forall n \in \mathbb{Z}^{\geq 3}.p(n)$. From Corollary 2, we can equivalently prove $p(3)$ and $\forall k \in \mathbb{Z}^{\geq 3}.\big(p(k) \longrightarrow p(k+1)\big)$. The induction basis states that the sum of the interior angles of every triangle is $(3-2)\cdot 180° = 180°$, a result from the theory of Euclidean geometry. For the induction step, assume that $p(k)$ holds for an arbitrary $k \in \mathbb{Z}^{\geq 3}$. Now, consider a convex $(k+1)$-vertex polygon. Take any three consecutive vertices in the polygon and draw a line from the first to the third. This line divides the polygon into a triangle and a convex k-vertex polygon. The sum of the interior angles of the two polygons is equal to the sum of the angles of the $(k+1)$-vertex polygon. Therefore, the sum of the angles in the $(k+1)$-vertex polygon is $180° + (k-2)\cdot 180° = \big((k+1)-2\big)\cdot 180°$.



Generalizations (Ctd.)

An alternative form of the mathematical induction, which is sometimes called the ***strong*** form of mathematical induction, is formulated as follows.

If α is a unary predicate on positive integers, then

$$\Big(\alpha(1) \wedge \forall k \in \mathbb{Z}^+.\big(\alpha(1) \wedge \alpha(2) \wedge \cdots \wedge \alpha(k) \longrightarrow \alpha(k+1)\big)\Big) \Longrightarrow \forall n \in \mathbb{Z}^+.\alpha(n).$$

Corollary 3. Let α be a unary predicate on $\mathbb{Z}^+$. Then,

$$\forall k \in \mathbb{Z}^+.\Big(\big(\forall m \in \mathbb{Z}^+.\big(m < k \longrightarrow \alpha(m)\big)\big) \longrightarrow \alpha(k)\Big) \Longrightarrow \forall n \in \mathbb{Z}^+.\alpha(n).$$

Proof. Let β be a predicate on positive integers defined by

$$\beta(n) \stackrel{\text{def}}{=} \forall m \in \mathbb{Z}^+.\big(m < n \longrightarrow \alpha(m)\big).$$

It is immediate that $\beta(1)$ is true. Now, for an arbitrary $k \in \mathbb{Z}^+$, we prove that $\beta(k)$ implies $\beta(k+1)$. Assume that $\beta(k)$ is true. From the assumption

$$\forall k \in \mathbb{Z}^+.\Big(\big(\forall m \in \mathbb{Z}^+.\big(m < k \longrightarrow \alpha(m)\big)\big) \longrightarrow \alpha(k)\Big),$$

it follows that $\alpha(k)$ is true. Thus, $\beta(k) \wedge \alpha(k)$ or, equivalently, $\beta(k+1)$ is true. Hence, by the proof principle of mathematical induction, $\forall n \in \mathbb{Z}^+.\beta(n)$. Consequently, $\forall n \in \mathbb{Z}^+.\alpha(n)$.

Generalizations (Ctd.)

Corollary 4. Let α be a unary predicate on $\mathbb{Z}^{\geq n_0}$. Then,

$$\forall k \in \mathbb{Z}^{\geq n_0}.\Big(\big(\forall m \in \mathbb{Z}^{\geq n_0}.\big(m < k \longrightarrow \alpha(m)\big)\big) \longrightarrow \alpha(k)\Big) \Longrightarrow \forall n \in \mathbb{Z}^{\geq n_0}.\alpha(n).$$

Example 4. Prove that every positive integer greater than 1 can be expressed in exactly one way, apart from rearrangement, as a product of one or more primes (the ***fundamental theorem of arithmetic***.)

Solution. Let $\alpha(n)$ be "n can be expressed in exactly one way as a product of one or more primes." We must prove that $\forall n \in \mathbb{Z}^{\geq 2}.\,\alpha(n)$. By Corollary 4, we can equivalently show that

$$\forall k \in \mathbb{Z}^{\geq 2}.\Big(\big(\forall m \in \mathbb{Z}^{\geq 2}.\big(m < k \longrightarrow \alpha(m)\big)\big) \longrightarrow \alpha(k)\Big).$$

Assume that k is an arbitrary element of $\mathbb{Z}^{\geq 2}$ and that

$$\big(\forall m \in \mathbb{Z}^{\geq 2}.\big(m < k \longrightarrow \alpha(m)\big)\big)$$

holds. If k is not prime and $k \geq 3$, it can be written as a product of two positive integers k_1 and k_2 where $k_1, k_2 \in \mathbb{Z}^{\geq 2}$. From the induction hypothesis, k_1 and k_2 can be expressed in exactly one way as a product of one or more primes. This establishes the truth of $\alpha(k)$. For $k = 2$, we should prove $\alpha(k)$ directly. This is immediate because 2 is prime.

Generalizations (Ctd.)

Example 5. Prove that every positive integer greater than or equal to 14 can be expressed as a sum of 3's and 8's.

Solution. Let $\alpha(n)$ be defined as

$$\exists r, s \in \mathbb{Z}^{\geq 0}. n = 3r + 8s.$$

We must prove that

$$\forall n \in \mathbb{Z}^{\geq 14}. \alpha(n).$$

By the generalization of the strong form of mathematical induction, we can equivalently show that

$$\forall k \in \mathbb{Z}^{\geq 14}. \Big(\big(\forall m \in \mathbb{Z}^{\geq 14}. \big(m < k \longrightarrow \alpha(m) \big) \big) \longrightarrow \alpha(k) \Big).$$

Assume that k is an arbitrary element of $\mathbb{Z}^{\geq 14}$ and that

$$\big(\forall m \in \mathbb{Z}^{\geq 14}. \big(m < k \longrightarrow \alpha(m) \big) \big)$$

holds. We can write $k = (k - 3) + 3$. If $k \geq 17$, we have $14 \leq k - 3 < k$. From the induction hypothesis, it then follows that $\exists r, s \in \mathbb{Z}^{\geq 0}. k - 3 = 3r + 8s$. Thus, $\exists r, s \in \mathbb{Z}^{\geq 0}. k = 3(r + 1) + 8s$. For $k = 14$, $k = 15$, and $k = 16$, we may directly establish the truth of $\alpha(k)$ as follows:

$$14 = 3 \cdot 2 + 8 \cdot 1.$$
$$15 = 3 \cdot 5 + 8 \cdot 0.$$
$$16 = 3 \cdot 0 + 8 \cdot 2.$$

Generalizations (Ctd.)

Can one use the principle of mathematical induction (also called ***induction on positive integers***) to prove properties of elements of other sets?

Suppose you are to prove that the predicate α is true of all elements of a set A, that is, $\forall x \in A.\, \alpha(x)$. You may take the following steps:

1. Find a function $f: A \longrightarrow \mathbb{Z}^+$.
2. Define $\beta(n) \stackrel{\text{def}}{=} \forall x \in A.\, \big(f(x) = n \longrightarrow \alpha(x)\big)$.
3. Prove that $\forall n \in \mathbb{Z}^+.\, \beta(n)$.

We have already used this technique. In one of the examples, we mapped the set of convex polygons to the set of the positive integers greater than or equal to 3 using the function $f: \mathbf{P} \longrightarrow \mathbb{Z}^{\geq 3}$ defined by

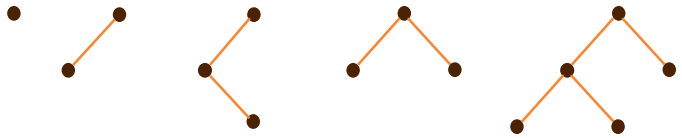
$$f(P) = \text{the number of vertices of } P,$$

where $\mathbf{P}$ is the set of all convex polygons.

We can always define a function from any set A to the set of positive integers (for example, one may define f as $f(x) = 1$ for every $x \in A$.) Of course, one function from A to $\mathbb{Z}^+$ might make it possible to prove the property we are interested in while another might not.

Generalizations (Ctd.)

Example 6. A ***binary tree*** is either empty, a leaf or an "internal node" with two subtrees. Some examples are shown below.



Prove that the number of leaves of any binary tree is at most one plus the number of internal nodes.

Solution. Let α be a predicate on the set $\mathcal{T}$ of binary trees defined by

$$\alpha(t) \stackrel{\text{def}}{=} leaves(t) \leq inodes(t) + 1,$$

where $leaves(t)$ and $inodes(t)$ are the number of leaves and internal nodes of the binary tree t, respectively. We must prove that $\forall t \in \mathcal{T}.\alpha(t)$. Define the function $height: \mathcal{T} \longrightarrow \mathbb{Z}^{\geq 0}$ that takes a binary tree to its height, that is, the length of the longest path from the root to the leaves. Define also the predicate β on $\mathbb{Z}^{\geq 0}$ as

$$\beta(n) \stackrel{\text{def}}{=} \forall t \in \mathcal{T}.\big(height(t) = n \longrightarrow \alpha(t)\big).$$

Now, we use the generalization of the strong form of mathematical induction and prove that $\forall n \in \mathbb{Z}^{\geq 0}.\beta(n)$. Assuming that $k \in \mathbb{Z}^{\geq 0}$, $k \geq 1$, and $\beta(m)$ is true of all $0 \leq m < k$ (the induction hypothesis), we show that $\beta(k)$ is true. That is, for all binary trees with $height(t) = k$, $leaves(t) \leq inodes(t) + 1$ holds. Any tree t with $height(t) = k \geq 1$ has two subtrees t_1 and t_2 where $0 \leq height(t_1), height(t_2) < k$. Thus, from the induction hypothesis, we have $leaves(t_1) \leq inodes(t_1) + 1$ and $leaves(t_2) \leq inodes(t_2) + 1$. Consequently,

$$leaves(t) = leaves(t_1) + leaves(t_2) \leq inodes(t_1) + 1 + inodes(t_2) + 1 = inodes(t) + 1.$$

We must also prove $\beta(0)$ directly, which is immediate.

Textbook: Ralph P. Grimaldi, Discrete and Combinatorial Mathematics

Do exercises of Chapter 4 as homework and upload your solutions via Moodle (follow the instructions on the page of the TA of this course.)