SC 612: Discrete Mathematics (MSc(IT)-Autumn 2023)

Lectures 6: Mathematical Induction

Instructor: Gopinath Panda *August 21, 2023*

1 Mathematical Induction

- Deductive reasoning uses rules of inference to draw conclusions from premises
- Inductive reasoning makes conclusions only supported, but not ensured, by evidence.
- Mathematical proofs, including arguments that use mathematical induction, are deductive, not inductive.

PRINCIPLE OF MATHEMATICAL INDUCTION:
To prove that $P(n)$ is true $\forall\ n$, where $P(n)$ is a propositional function,
we complete two steps:
BASIS STEP: Verify that $P(1)$ is true.
INDUCTIVE STEP: $P(k) \to P(k+1)$ is true for all positive integers k.

- To complete the inductive step of a proof using the principle of mathematical induction,

1. we assume that $P(k)$ is true for an arbitrary positive integer k and

2. show that under this assumption, $P(k+1)$ must also be true.

The assumption that $P(k)$ is true is called the inductive hypothesis.
Once we complete both steps, we have shown that $\forall n P(n)$ is true.
$\forall k(P(k) \to P(k+1))$ is true.

Expressed as a rule of inference,

$$(P(1) \wedge \forall k(P(k) \to P(k+1))) \to \forall n P(n),$$

Remark:
- It is not assumed that $P(k)$ is true for all positive integers!
- It is only shown that if it is assumed that $P(k)$ is true, then $P(k+1)$ is also true.

Thus, a proof by mathematical induction is not a case of circular reasoning.

Validity of Mathematical Induction Why is mathematical induction a valid proof technique? The reason comes from the well-ordering property (an axiom for the set of positive integers).
- every nonempty subset of the set of positive integers has a least element.

Suppose we know that $P(1)$ is true and that the proposition $P(k) \to P(k+1)$ is true for all positive integers k.
<u>To show that</u> $P(n)$ must be true for all positive integers n.

If not assume that there is at least one positive integer for which $P(n)$ is false.
$S=$ {n: $P(n)$ is false} is nonempty, because at least $|S| = 1$.
Thus, by the well-ordering property, S has a least element, say m.
$m \neq 1$, because $P(1)$ is true $\implies$ $m-1$ is a positive integer.
Furthermore, because $m-1 < m$, it is not in S, otherwise m won't be the least element.

Thus, $P(m-1)$ must be true.
Because the conditional statement $P(m-1) \to P(m)$ is also true, it must be the case that $P(m)$ is true.
This contradicts the choice of m.
Hence, $P(n)$ must be true for every positive integer n.

Example. *Show that if n is a positive integer, then*

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

Solution: Let $P(n)$: sum of the first n positive integers, $1+2+\cdots n = \frac{n(n+1)}{2}$, is $n(n+1)/2$.
To prove that $P(n)$ is true for $n = 1, 2, 3, \ldots$, we have
Basis Step: verify $P(1)$ is true and
Inductive step: $P(k)$ implies $P(k+1)$ is true for $k = 1, 2, 3, \ldots$.
BASIS STEP: $P(1)$ is true, because $1 = \frac{1(1+1)}{2}$.
INDUCTIVE STEP: Suppose $P(k)$ holds for an arbitrary positive integer k. That is,

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Under this assumption, <u>To show</u> $P(k+1)$ is true, namely, that

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)[(k+1)+1]}{2} = \frac{(k+1)(k+2)}{2}$$

is also true. When we add $k+1$ to both sides of the equation in $P(k)$, we obtain

$$\begin{aligned}1 + 2 + \cdots + k + (k+1) &\overset{\text{IH}}{=} \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

Therefore, $P(k+1)$ is true under the assumption that $P(k)$ is true.
We have completed the basis step and the inductive step, so by mathematical induction $P(n)$ is true for all positive integers n.

Example. *Use mathematical induction to show that*

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all non-negative integers n.

Solution: Let $P(n)$: $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for the integer n.
BASIS STEP: $P(0)$ is true because $2^0 = 1 = 2^1 - 1$.
INDUCTIVE STEP: For the inductive hypothesis, suppose $P(k)$ is true for an arbitrary non-negative integer k. That is, we assume that

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1.$$

To show that $P(k+1)$ is also true. That is, we must show that

$$1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} = 2^{(k+1)+1} - 1 = 2^{k+2} - 1$$

assuming the inductive hypothesis $P(k)$. Under the assumption of $P(k)$, we see that

$$\begin{aligned} 1+2+2^2+\cdots+2^k+2^{k+1} &= \left(1+2+2^2+\cdots+2^k\right)+2^{k+1} \\ &\overset{\text{IH}}{=} \left(2^{k+1}-1\right)+2^{k+1} \\ &= 2\cdot 2^{k+1}-1 \\ &= 2^{k+2}-1. \end{aligned}$$

By mathematical induction, $P(n)$ is true for all non-negative integers n.
That is, $1+2+\cdots+2^n = 2^{n+1}-1$ for all non-negative integers n.

Example. *Use mathematical induction to prove that $2^n < n\,!$ for every integer n with $n \geq 4$. (Note that this inequality is false for $n = 1, 2,$ and 3 .)*

Solution: Let $P(n)$ be the proposition that $2^n < n!$.
BASIS STEP: To prove the inequality for $n \geq 4$ requires that the basis step be $P(4)$. Note that $P(4)$ is true, because $2^4 = 16 < 24 = 4\,!$
INDUCTIVE STEP: For the inductive step, suppose $P(k)$ is true for an arbitrary integer k with $k \geq 4$. That is, $2^k < k\,!$ for the positive integer k with $k \geq 4$.
To show $P(k+1)$ is true under this hypothesis.
That is, we must show that if $2^k < k!$ for an arbitrary positive integer k where $k \geq 4$, then $2^{k+1} < (k+1)\,!$. We have

$$\begin{aligned} 2^{k+1} &= 2\cdot 2^k && \text{by definition of exponent} \\ &< 2\cdot k! && \text{by the inductive hypothesis} \\ &< (k+1)k! && \text{because } 2 < k+1 \\ &= (k+1)! && \text{by definition of factorial function.} \end{aligned}$$

Thus, $P(k+1)$ is true when $P(k)$ is true. This completes the inductive step of the proof. We have completed the basis step and the inductive step. Hence, by mathematical induction $P(n)$ is true for all integers n with $n \geq 4$. That is, we have proved that $2^n < n!$ is true for all integers n with $n \geq 4$.

2 STRONG INDUCTION

To prove that $P(n)$ is true for all positive integers n, we complete two steps:
BASIS STEP: Verify that $P(1)$ is true.
INDUCTIVE STEP: Show that the conditional statement

$$[P(1) \wedge P(2) \wedge \cdots \wedge P(k)] \rightarrow P(k+1)$$

is true for all positive integers k.
Note: Inductive hypothesis for Strong Induction: $P(j)$ is true for $j = 1, 2, \ldots, k$.
Inductive hypothesis for Mathematical Induction: $P(k)$ is true.

- mathematical induction and strong induction are equivalent.
- That is, any proof using mathematical induction can also be considered to be a proof by strong induction because the inductive hypothesis of a proof by mathematical induction is part of the inductive hypothesis in a proof by strong induction.
- Strong induction is sometimes called the second principle of mathematical induction or complete induction.

Example. *Show that if n is an integer greater than 1 , then n can be written as the product of primes.*

Solution: Let $P(n)$ be the proposition that n can be written as the product of primes.
BASIS STEP: $P(2)$ is true, because 2 can be written as the product of one prime, itself.
INDUCTIVE STEP: The inductive hypothesis is the assumption that $P(j)$ is true for all integers j with $2 \leq j \leq k$, that is,
the assumption that j can be written as the product of primes whenever j is a positive integer at least 2 and not exceeding k.
To show that $P(k+1)$ is true, that is, $k+1$ is the product of primes.
There are two cases to consider, namely, when $k+1$ is prime and when $k+1$ is composite.
If $k+1$ is prime, we immediately see that $P(k+1)$ is true.
If $k+1$ is composite it can be written as the product of two positive integers a and b with $2 \leq a \leq b < k+1$. Because both a and b are integers at least 2 and not exceeding k, we can use the inductive hypothesis, both a and b are product of primes.
Thus, if $k+1$ is composite, it can be written as the product of primes, namely, those primes in the factorization of a and those in the factorization of b.

3 Recursive Definition

Recursion is the process of defining an object in terms of itself, when it is difficult to define that explicitly.
- Recursion can be used to define sequences, functions, and sets.

3.1 Recursively defined functions

We use two steps to define a function with the set of nonnegative integers as its domain:

- BASIS STEP: Specify the value of the function at zero.

- RECURSIVE STEP: Define a rule for finding its value at an integer from its previous values

Example. *Suppose that f is defined recursively by*

$$\begin{aligned} f(0) &= 3 \\ f(n+1) &= 2f(n)+3 \end{aligned}$$

Find $f(1), f(2), f(3)$, and $f(4)$.

Solution: From the recursive definition it follows that

$$\begin{aligned} f(1) &= 2f(0)+3 = 2\cdot 3+3 = 9, \\ f(2) &= 2f(1)+3 = 2\cdot 9+3 = 21, \\ f(3) &= 2f(2)+3 = 2\cdot 21+3 = 45, \\ f(4) &= 2f(3)+3 = 2\cdot 45+3 = 93. \end{aligned}$$

Recursively defined functions are well defined. That is, for every positive integer, the value of the function at this integer is determined in an unambiguous way.

Example. *Give a recursive definition of a^n, where a is a nonzero real number and n is a non-negative integer.*

Solution:
- Basis step: $a^0 = 1$.
- Recursive step: $a^{n+1} = a \cdot a^n$, for $n = 0, 1, 2, 3, \ldots$ These two equations uniquely define a^n for all nonnegative integers n.

Example. *Give a recursive definition of*

$$\sum_{k=0}^{n} a_k$$

Solution:
- Basis step: $\sum_{k=0}^{0} a_k = a_0$
- Recursive step: $\sum_{k=0}^{n+1} a_k = (\sum_{k=0}^{n} a_k) + a_{n+1}$

Example. *Show that whenever* $n \geq 3, f_n > \alpha^{n-2}$, *where* $\alpha = (1+\sqrt{5})/2$. *That is, Fibonacci numbers grow faster than a geometric series with common ratio* $\alpha = (1+\sqrt{5})/2$.

Solution: We can use strong induction to prove this inequality.
Let $P(n) : f_n > \alpha^{n-2}$.
To show: $P(n)$ is true whenever n is an integer greater than or equal to 3, where f_n are Fibonacci numbers given by $f_0 = 0, f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$.
- BASIS STEP: First, note that

for $n = 3$, $f_3 = 2 > (1+\sqrt{5})/2 = \alpha$, so $P(3)$ is true.
for $n = 4$, $f_4 = 3 > (3+\sqrt{5})/2 = \alpha^2$, so $P(4)$ are true.
- INDUCTIVE STEP: Assume that $P(j)$ is true, i.e., $f_j > \alpha^{j-2}$, for all integers j with $3 \leq j \leq k$, where $k \geq 4$.

To show $P(k+1)$ is true, that is, $f_{k+1} > \alpha^{k-1}$.
Because α is a solution of $x^2 - x - 1 = 0$ (as the quadratic formula shows), it follows that $\alpha^2 = \alpha + 1$. Therefore,

$$\alpha^{k-1} = \alpha^2 \cdot \alpha^{k-3} = (\alpha+1)\alpha^{k-3} = \alpha \cdot \alpha^{k-3} + 1 \cdot \alpha^{k-3} = \alpha^{k-2} + \alpha^{k-3}.$$

By the inductive hypothesis, because $k \geq 4$, we have

$$f_{k-1} > \alpha^{k-3}, \quad f_k > \alpha^{k-2}.$$

Therefore, it follows that

$$f_{k+1} = f_k + f_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}.$$

Hence, $P(k+1)$ is true.

3.2 Recursively defined sets

Example. *Consider the subset S of the set of integers recursively defined by*
BASIS STEP: $3 \in S$.
RECURSIVE STEP: If $x \in S$ and $y \in S$, then $x + y \in S$.
The new elements found to be in S are 3 by the basis step, $3+3 = 6$ at the first application of the recursive step, $3+6 = 6+3 = 9$ and $6+6 = 12$ at the second application of the recursive step, and so on.
S is the set of all positive multiples of 3.

Applications: study of strings

The set Σ^* of strings over the alphabet Σ is defined recursively by
- BASIS STEP: $\lambda \in \Sigma^*$ (where λ is the empty string containing no symbols).
- RECURSIVE STEP: If $w \in \Sigma^*$ and $x \in \Sigma$, then $wx \in \Sigma^*$

Two strings can be combined via the operation of concatenation. Let Σ be a set of symbols and Σ^* the set of strings formed from symbols in Σ. We can define the concatenation of two strings, denoted by $\cdot$, recursively as follows.
- BASIS STEP: If $w \in \Sigma^*$, then $w \cdot \lambda = w$, where λ is the empty string.
- RECURSIVE STEP: If $w_1 \in \Sigma^*$ and $w_2 \in \Sigma^*$ and $x \in \Sigma$, then $w_1 \cdot (w_2 x) = (w_1 \cdot w_2)\, x$.

The concatenation of the strings w_1 and w_2 is often written as $w_1 w_2$ rather than $w_1 \cdot w_2$. By repeated application of the recursive definition, it follows that the concatenation of two strings w_1 and w_2 consists of the symbols in w_1 followed by the symbols in w_2. For instance, the concatenation of $w_1 =$ abra and $w_2 =$ cadabra is $w_1 w_2 =$ abracadabra.

Length of a String Give a recursive definition of $l(w)$, the length of the string w. Solution: The length of a string can be recursively defined by

$$l(\lambda) = 0$$
$$l(wx) = l(w) + 1 \text{ if } w \in \Sigma^* \text{ and } x \in \Sigma.$$

4 Structural Induction

This is a method to prove results about recursively defined sets. It consists of two steps:
- Basis step: specify some initial elements
- Recursive step: define a rule for constructing new elements from the basis step.

To prove results about recursively defined sets, we generally use some form of mathematical induction.

Example. *Show that the set S of all positive integers that are multiples of 3, that is: $3 \in S$ and that if $x \in S$ and $y \in S$, then $x + y \in S$.*

Solution: Let A be the set of all positive integers divisible by 3 .
To prove that $A = S$, we must show that
- A is a subset of S and
- S is a subset of A.

To prove that $A \subseteq S$, we must show that every positive integer divisible by 3 is in S. We will use mathematical induction to prove this.
Let $P(n) : 3n \in S$.
Basis step: holds because by the first part of the recursive definition of $S, 3 \cdot 1 = 3$ is in S.
Inductive step: assume that $P(k)$ is true, namely, that $3k$ is in S. Because $3k$ is in S and because 3 is in S, it follows from the second part of the recursive definition of S that $3k + 3 = 3(k + 1)$ is also in S.
To prove that S is a subset of A, we use the recursive definition of S.
Basis step: 3 is in S. Because $3 = 3 \cdot 1$, all elements specified to be in S in this step are divisible by 3 and are therefore in A.

To show that all integers in S generated using the second part of the recursive definition are in A.
That is to show $x + y \in A$ whenever $x, y \in S$ also assumed to be in A.
Now if x and y are both in A, it follows that $3 \mid x$ and $3 \mid y$. it follows that $3 \mid x + y$. Hence, $x + y \in A$

5 Generalized Induction*

We can extend mathematical induction to prove results about other sets that have the well ordering property besides the set of integers.