# CSC165
# Mathematical Expression and Reasoning for Computer Science

**Module 12**

## Proof by Induction

## Mathematical Induction

- It is a method of mathematical proof used to establish a given statement is true for all (or subset of) natural numbers
- It is a form of direct proof, and it is done in two steps
- The first step, known as the basis (or base) step/case:
  - Prove the given statement for the first natural number
- The second step, known as the inductive step:
  - Prove that the given statement for any natural number (is true) implies the statement is true for the next natural number
- We infer that the given statement is established for all natural numbers

 

## Mathematical Induction

- Mathematical induction can be illustrated by the sequential effect of falling dominoes
- Imagine an infinite collection of dominos positioned one behind the other
- If one domino falls backward, it makes the domino after it falls backward as well
- If the first domino falls, all dominos fall

 

## Proof by Induction

- Consider the statement "$P(n)$ is true for all natural numbers $\geq a$"
- $\forall n \in \mathbb{N}: [(n \geq a) \rightarrow P(n)]$
- To prove this statement by induction:
  - Basis step: show that $P(a)$ is true
  - Inductive step: show that for all natural numbers $k \geq a$, if $P(k)$ is true, then $P(k+1)$ is true
- This is equivalent to proving

$P(a) \wedge (\forall k \in \mathbb{N}: [(k \geq a) \rightarrow (P(k) \rightarrow P(k+1))])$



## Proof Structure

- Prove $\forall n \in \mathbb{N}: [(n \geq a) \rightarrow P(n)]$
- Generic Proof:

Basis step: Prove $P(a)$

$\vdots$

Then $P(a)$.

Inductive step: Prove $\forall k \in \mathbb{N}: [k \geq a \rightarrow (P(k) \rightarrow P(k+1))]$

Let $k \in \mathbb{N}$.

Assume $k \geq a$.

Assume $P(k)$.

$\vdots$

Then $P(k+1)$.

Then $P(k) \rightarrow P(k+1)$.

Then $\forall k \in \mathbb{N}: [(k \geq a) \rightarrow (P(k) \rightarrow P(k+1))]$.

Therefore, $\forall n \in \mathbb{N}: [(n \geq a) \rightarrow P(n)]$.

# Example

- Use mathematical induction to prove "$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all natural numbers $n \geq 1$"
- Remember $\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$
- Using the generic form $\forall n \in \mathbb{N}: [n \geq a \rightarrow P(n)]$:
  - $a = 1$
  - $P(n): \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
- Prove $\forall n \in \mathbb{N}: \left[(n \geq 1) \rightarrow \left(\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\right)\right]$
- Basis step: prove $P(1)$
  - $\sum_{i=1}^{1} i = 1$
  - $\frac{1(1+1)}{2} = 1$
  - $P(1)$ is true





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

- Inductive step: prove $\forall k \in \mathbb{N}: [(k \geq 1) \rightarrow (P(k) \rightarrow P(k+1))]$
  - $P(k): \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$
  - $P(k+1): \sum_{i=1}^{k+1} i = \frac{(k+1)(k+1+1)}{2}$
  - Prove that for $k \geq 1$, if $P(k)$ is true, then $P(k+1)$ is true
  - Assume $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$
  - Then $\sum_{i=1}^{k+1} i = 1 + \cdots + k + (k+1) = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$
  - Then $\sum_{i=1}^{k+1} i = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}$
  - Then $P(k+1)$ is true

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

Basis step: Prove $P(1)$

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

Then $P(1)$.

Inductive step: Prove $\forall k \in \mathbb{N}: [(k \geq 1) \to (P(k) \to P(k+1))]$

Let $k \in \mathbb{N}$.

Assume $k \geq 1$.

Assume $P(k)$.

Then $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$.

Then $\sum_{i=1}^{k+1} i = 1 + \cdots + k + (k+1) \quad = \sum_{i=1}^{k} i + (k+1)$

…





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

…

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

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

$= \frac{k^2+3k+2}{2}$

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

Then $P(k+1)$.

Then $P(k) \to P(k+1)$.

Then $\forall k \in \mathbb{N}: [(k \geq 1) \to (P(k) \to P(k+1))]$.

Therefore, $\forall n \in \mathbb{N}: \left[(n \geq 1) \to \left(\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\right)\right]$.

## Example

- Prove $\forall n \in \mathbb{N}: \sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$ for all real numbers $r$ (where $r \neq 1$)

- $\sum_{i=0}^{n} r^i = r^0 + r^1 + \cdots + r^n$
- $P(n) = \sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$
- Basis step: prove $P(0)$
  - $\sum_{i=0}^{0} r^i = r^0 = 1$
  - $\frac{r^{0+1}-1}{r-1} = \frac{r^1-1}{r-1} = 1$
  - $P(0)$ is true



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

- Inductive step: prove $\forall k \in \mathbb{N}: [(k \geq 0) \rightarrow (P(k) \rightarrow P(k+1))]$
  - $P(k): \sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$
  - $P(k+1): \sum_{i=0}^{k+1} r^i = \frac{r^{k+2}-1}{r-1}$
  - Prove $\forall k \in \mathbb{N}: [P(k) \rightarrow P(k+1)]$
  - Assume $P(k)$ is true
  - Then $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$ is true
  - Then $\sum_{i=0}^{k+1} r^i = \sum_{i=0}^{k} r^i + r^{k+1} = \frac{r^{k+1}-1}{r-1} + r^{k+1}$
  - Then $\sum_{i=0}^{k+1} r^i = \frac{r^{k+1}-1}{r-1} + \frac{r^{k+1}(r-1)}{r-1} = \frac{(r^{k+1}-1)+r^{k+1}(r-1)}{r-1}$
  - Then $\sum_{i=0}^{k+1} r^i = \frac{r^{k+1}-1+r^{k+2}-r^{k+1}}{r-1} = \frac{r^{k+2}-1}{r-1}$
  - Then $P(k+1)$ is true

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

Basis step: Prove $P(0)$

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

Then $P(0)$.

Inductive step: Prove $\forall k \in \mathbb{N}: [P(k) \rightarrow P(k+1)]$

Let $k \in \mathbb{N}$.

Assume $P(k)$.

Then $\sum_{i=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}$.

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

$= \frac{r^{k+1}-1}{r-1} + r^{k+1}$

…

 13

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

….

$= \frac{r^{k+1}-1}{r-1} + \frac{r^{k+1}(r-1)}{r-1}$

$= \frac{(r^{k+1}-1)+r^{k+1}(r-1)}{r-1}$

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

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

Then $P(k+1)$.

Then $P(k) \rightarrow P(k+1)$.

Then $\forall k \in \mathbb{N}: [P(k) \rightarrow P(k+1)]$.

Therefore, $\forall n \in \mathbb{N}: \left[\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}\right]$.

 14

## Example

- Prove $\forall n \in \mathbb{N}: 2^{2n} - 1$ is divisible by 3
- $P(n)$: $2^{2n} - 1$ is divisible by 3
- $2^{2n} - 1$ divisible by 3$\leftrightarrow \exists j \in \mathbb{N}: 2^{2n} - 1 = 3j$
- Basis step: prove $P(0)$
  - $2^{2(0)} - 1 = 1 - 1 = 0$
  - 0 is divisible by 3 (i.e., $\exists j \in \mathbb{N}: 0 = 3j$)
  - $P(0)$ is true





## Prove: $2^{2n} - 1$ is divisible by 3

- Inductive step: prove $\forall k \in \mathbb{N}: [P(k) \rightarrow P(k+1)]$
  - $P(k)$: $2^{2k} - 1$ is divisible by 3
  - $P(k+1)$: $2^{2(k+1)} - 1$ is divisible by 3
  - Assume $P(k)$ is true
  - Then $2^{2k} - 1$ is divisible by 3 is true
  - Then $\exists j \in \mathbb{N}: 2^{2k} - 1 = 3j$
  - Let $j_0 \in \mathbb{N}$ such that $2^{2k} - 1 = 3j_0$
  - Then $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^{2k}(2^2) - 1$
  - Then $2^{2(k+1)} - 1 = 2^{2k}(4) - 1 = 2^{2k}(3+1) - 1$
  - Then $2^{2(k+1)} - 1 = 2^{2k}(3) + (2^{2k} - 1) = 2^{2k}(3) + 3j_0$
  - Then $2^{2(k+1)} - 1 = 3(2^{2k} + j_0)$
  - Then $2^{2(k+1)} - 1$ is divisible by 3
  - Then $P(k+1)$ is true

# Proof: $2^{2n} - 1$ is divisible by 3

Basis step: Prove $P(0)$

$2^{2(0)} - 1 = 1 - 1 = 0.$

Then $\exists j \in \mathbb{N}: 0 = 3j.$

Then $P(0)$.

Inductive step: Prove $\forall k \in \mathbb{N}: [P(k) \rightarrow P(k+1)]$

Let $k \in \mathbb{N}$.

Assume $P(k)$.

Then $2^{2k} - 1$ is divisible by 3.

Then $\exists j \in \mathbb{N}: 2^{2k} - 1 = 3j.$

Let $j_0 \in \mathbb{N}$ such that $2^{2k} - 1 = 3j_0$.

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

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

$= 2^{2k}(4) - 1$

...




# Proof: $2^{2n} - 1$ is divisible by 3

....

$= 2^{2k}(3 + 1) - 1$

$= 2^{2k}(3) + \left(2^{2k} - 1\right)$

$= 2^{2k}(3) + 3j_0$

$= 3\left(2^{2k} + j_0\right).$

Let $j_1 = 2^{2k} + j_0$.

Then $j_1 \in \mathbb{N}$.

Then $2^{2(k+1)} - 1 = 3j_1$.

Then $\exists j \in \mathbb{N}: 2^{2(k+1)} - 1 = 3j.$

Then $2^{2(k+1)} - 1$ is divisible by 3.

Then $P(k+1)$.

Then $P(k) \rightarrow P(k+1)$.

Then $\forall k \in \mathbb{N}: [P(k) \rightarrow P(k+1)].$

Therefore, $\forall n \in \mathbb{N}: 2^{2n} - 1$ is divisible by 3.

## Example

- Prove $\forall n \in \mathbb{N}: [(n \geq 3) \rightarrow (2n + 1 < 2^n)]$
- $P(n): 2n + 1 < 2^n$
- Basis step: prove $P(3)$
  - $2(3) + 1 = 7 < 2^3 = 8$
  - $P(3)$ is true
- Inductive step: prove $\forall k \in \mathbb{N}: [(k \geq 3) \rightarrow (P(k) \rightarrow P(k+1))]$
  - $P(k): 2k + 1 < 2^k$
  - $P(k+1): 2(k+1) + 1 < 2^{k+1}$
  - Assume $P(k)$ is true
  - Then $2k + 1 < 2^k$ is true
  - Then $2(k+1) + 1 = 2k + 3 = (2k+1) + 2$
  - Then $2(k+1) + 1 < 2^k + 2 < 2^k(2)$
  - Then $2(k+1) + 1 < 2^k 2^1 = 2^{k+1}$
  - Then $P(k+1)$ is true




## Proof: $\forall n \in \mathbb{N}: [(n \geq 3) \rightarrow (2n + 1 < 2^n)]$

Basis step: Prove $P(3)$

  $2(3) + 1 = 7 < 2^3 = 8.$

  Then $P(3)$.

Inductive step: Prove $\forall k \in \mathbb{N}: [(k \geq 3) \rightarrow (P(k) \rightarrow P(k+1))]$

  Let $k \in \mathbb{N}$.

    Assume $k \geq 3$.

      Assume $P(k)$.

        Then $2k + 1 < 2^k$.

        Then $2(k+1) + 1 = 2k + 3$

        $= (2k+1) + 2.$

        …

# Proof: $\forall n \in \mathbb{N}: [(n \geq 3) \rightarrow (2n + 1 < 2^n)]$

....

Then $2(k+1) + 1 < 2^k + 2$
$< 2^k(2)$ # since $2^k \geq 8$, $2^k + 2 < 2\ 2^k$
$= 2^k 2^1$
$= 2^{k+1}$. # $2(k+1) + 1 < 2^{k+1}$

Then $P(k+1)$.

Then $P(k) \rightarrow P(k+1)$.

Then $\forall k \in \mathbb{N}: [(k \geq 3) \rightarrow (P(k) \rightarrow P(k+1))]$.

Therefore, $\forall n \in \mathbb{N}: [(n \geq 3) \rightarrow (2n + 1 < 2^n)]$.

 

# Paradox

- An example of a wrong proof
- Prove "All sheep have the same color"
- Basis step:
  - If there is only one sheep, there is only one color
- Inductive step:
  - Assume that within any set of $k$ sheep, there is only one color
  - Consider any set of $k + 1$ sheep. Number them as: $1, 2, 3, \ldots, k, k + 1$
  - Consider the sets $\{1, 2, 3, \ldots, k\}$ and $\{2, 3, 4, \ldots, k + 1\}$
  - Each is a set of only $k$ sheep, therefore within each set there is only one color (as assumed)
  - The two sets overlap, so there must be only one color among all $k + 1$ sheep
- Therefore, in any group of sheep, all sheep must have the same color!
- What do you think? What is wrong with this proof?

 

# Strong Induction

 

## Strong Induction

- The Principle of Mathematical Induction asserts that the conjunction of "the base case $P(a)$" being true and "$P(k)$ implies $P(k+1)$" is true for all $k$, implies $P(n)$ is true for all $n$
- However, sometimes we need to "look" further back than 1 step to obtain $P(k+1)$
- That is where the Strong Form of Mathematical Induction comes in useful
- Principle of Strong Mathematical Induction:
  - Let $P(n)$ be a predicate defined over integers $n$
  - Let $a$ and $b$ be fixed integers with $a \leq b$
  - Suppose the following two statements are true:
    - $P(a), P(a+1), \ldots, P(b)$ are all true (Basis step)
    - For any integer $k \geq b$, if $P(i)$ is true for all integers $i$ with $a \leq i \leq k$, then $P(k+1)$ is true (Inductive step)
  - Then the statement $P(n)$ is true for all integers $n \geq a$

 

# Proof Structure

- Prove $\forall n \in \mathbb{N}: [(n \geq a) \rightarrow P(n)]$
- Generic Proof:

Basis step: Prove $P(a), P(a+1) \dots P(b)$

$\vdots$

Then $P(a)$.

$\vdots$

Then $P(b)$.

Inductive step: Prove $\forall k \in \mathbb{N}: \left[k \geq b \rightarrow \left(\left(\forall i \in \{a, a+1, \dots, k\}: P(i)\right) \rightarrow P(k+1)\right)\right]$

Let $k \in \mathbb{N}$. Assume $k \geq b$.

Assume $\forall i \in \{a, a+1, \dots, k\}: P(i)$.

$\vdots$

Then $P(k+1)$.

Then $\left(\forall i \in \{a, a+1, \dots, k\}: P(i)\right) \rightarrow P(k+1)$.

Then $\forall k \in \mathbb{N}: \left[k \geq b \rightarrow \left(\left(\forall i \in \{a, a+1, \dots, k\}: P(i)\right) \rightarrow P(k+1)\right)\right]$.

Therefore, $\forall n \in \mathbb{N}: [(n \geq a) \rightarrow P(n)]$.





# Example

- Define a sequence $s_0, s_1, s_2, \dots$ as:

$s_0 = 0, s_1 = 4$, and $s_k = 6s_{k-1} - 5s_{k-2}$ for all integers $k \geq 2$

- Prove that $\forall n \in \mathbb{N}: s_n = 5^n - 1$
- Thoughts:
  - $s_0 = 0, s_1 = 4$
  - $s_2 = 6s_1 - 5s_0 = 24 = 5^2 - 1$
  - $s_3 = 6s_2 - 5s_1 = 144 - 20 = 124 = 5^3 - 1$
- Base case:
  - Show $P(0)$ and $P(1)$
  - $s_0 = 0 = 5^0 - 1$
  - $s_1 = 4 = 5^1 - 1$

# Example

- Inductive case:
  - For $k \geq b = 1$: if $P(i)$ is true for $a = 0 \leq i \leq k$, show that $P(k+1)$ is true
  - Let $k \geq 1$
  - Assume $s_i = 5^i - 1$ for all integers $i$ such that $0 \leq i \leq k$
  - Show $s_{k+1} = 5^{k+1} - 1$
  - $s_{k+1} = 6s_k - 5s_{k-1} = 6\left(5^k - 1\right) - 5\left(5^{k-1} - 1\right)$
  - $s_{k+1} = (6)5^k - 6 - 5^k + 5 = (6-1)5^k - 1$
  - $s_{k+1} = (5)5^k - 1 = 5^{k+1} - 1$




# Proof: $\forall n \in \mathbb{N}: s_n = 5^n - 1$

Basis step: Prove $P(0), P(1)$

$s_0 = 0 = 5^0 - 1.$

Then $P(0)$.

$s_1 = 4 = 5^1 - 1.$

Then $P(1)$

Inductive step: Prove $\forall k \in \mathbb{N}: \left[k \geq 1 \rightarrow \left(\left(\forall i \in \{0, \dots, k\}: P(i)\right) \rightarrow P(k+1)\right)\right]$

Let $k \in \mathbb{N}$.

Assume $k \geq 1$.

Assume $\forall i \in \{0, \dots, k\}: P(i)$. $\quad \#P(i){:}\ s_i = 5^i - 1$

Then $k - 1 \geq 0$.

Then $s_{k+1} = 6s_k - 5s_{k-1} = 6\left(5^k - 1\right) - 5\left(5^{k-1} - 1\right)$

$= (6)5^k - 6 - 5^k + 5 = (6-1)5^k - 1 = (5)5^k - 1 = 5^{k+1} - 1.$

Then $P(k+1)$.

Then $\left(\forall i \in \{0, \dots, k\}: P(i)\right) \rightarrow P(k+1)$.

Then $k \geq 1 \rightarrow \left(\left(\forall i \in \{0, \dots, k\}: P(i)\right) \rightarrow P(k+1)\right)$.

Then $\forall k \in \mathbb{N}: \left[k \geq 1 \rightarrow \left(\left(\forall i \in \{0, \dots, k\}: P(i)\right) \rightarrow P(k+1)\right)\right]$.

Therefore, $\forall n \in \mathbb{N}: s_n = 5^n - 1$.