# CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Aug 10, 2023

Lecture 03 – Induction and Well Ordering Principle

# Interesting fallacy in using induction!

**Conjecture: All horses have the same colour.**

"Proof" by induction on number of horses:

1. Base Case ($n = 1$) The case with one horse is trivial.
2. Induction Hypothesis Assume for $n = k \geq 1$, i.e., any set of $k (\geq 1)$ horses has same color.
3. Induction Step We want to show any set of $k + 1$ horses have same color. Consider such a set, say $1, \ldots, k + 1$.
   - (A) First, consider horses $1, \ldots, k$. By induction hypothesis, they have same color.
   - (B) Next, consider horses $2, \ldots, k + 1$. By induction hypothesis, they have same color.
   - (C) Therefore, 1 has same color as 2 (by A) and 2 has same color as $k + 1$ (by B), implies all $k + 1$ have same color.
4. Thus, by induction, we conclude that for all $n \geq 1$, any set of $n$ horses has the same color. $\square$

Where is the bug?

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction:

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n-1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n-1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

1. Base case:

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n-1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

1. Base case: if $n = 0$, $f(a, 0) = 1 = a^0$.

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n-1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

1. Base case: if $n = 0$, $f(a, 0) = 1 = a^0$.
2. Induction Hyp:

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

1. Base case: if $n = 0$, $f(a, 0) = 1 = a^0$.
2. Induction Hyp: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n-1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

1. Base case: if $n = 0$, $f(a, 0) = 1 = a^0$.
2. Induction Hyp: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.
3. Induction Step:

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n - 1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

1. Base case: if $n = 0$, $f(a, 0) = 1 = a^0$.
2. Induction Hyp: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.
3. Induction Step: For $n = k + 1$, $f(a, k + 1) = a \cdot f(a, k) = a \cdot a^k = a^{k+1}$ (by Induction Hyp).

# Proof of algorithm using induction

Consider the following algorithm:

**input:** non-zero real number $a$, non-negative integer $n$.

**procedure:** if $n = 0$, then return $f(a, n) = 1$;

else $f(a, n) = a \cdot f(a, n-1)$;

Theorem: Prove that the algorithm computes the function $f(a, n) = a^n$ for all non-negative integers $n$, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction: Fix an arbitrary non-zero real number $a$.

1. Base case: if $n = 0$, $f(a, 0) = 1 = a^0$.
2. Induction Hyp: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.
3. Induction Step: For $n = k + 1$, $f(a, k+1) = a \cdot f(a, k) = a \cdot a^k = a^{k+1}$ (by Induction Hyp).
4. Thus, by induction for all non-negative integers $n$, the algorithm above computes $f(a, n) = a^n$. □

# What is the basis for induction

**Axiom: Induction**

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

# What is the basis for induction

**Axiom: Induction**

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

**Theorem: Well Ordering Principle**

Every nonempty set of non-negative integers has a smallest element.

# What is the basis for induction

**Axiom: Induction**

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

**Theorem: Well Ordering Principle**

Every nonempty set of non-negative integers has a smallest element. Does this seem familiar? Obvious? What about for rationals?!

# What is the basis for induction

**Axiom: Induction**

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

**Theorem: Well Ordering Principle**

Every nonempty set of non-negative integers has a smallest element.

Prove it! (H.W)

# What is the basis for induction

**Axiom: Induction**

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

**Theorem: Well Ordering Principle**

Every nonempty set of non-negative integers has a smallest element.

Prove it! (H.W)

What about it's converse?

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

1. Suppose Induction is not true. This means that,
   1.1 Base Case holds: $P(0)$ is true;
   1.2 Induction Step holds: for $\forall n \geq 0$, $P(n) \implies P(n+1)$;
   1.3 But the conclusion doesn't hold, i.e., it isn't the case that ($P(n)$ is true for all non-negative integers).

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

1. Suppose Induction is not true. This means that,
   1.1 Base Case holds: $P(0)$ is true;
   1.2 Induction Step holds: for $\forall n \geq 0$, $P(n) \implies P(n+1)$;
   1.3 But the conclusion doesn't hold, i.e., it isn't the case that ($P(n)$ is true for all non-negative integers).
2. Point (1.3) implies there exists $n \in \mathbb{N}$ s.t., $P(n)$ is false.

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

1. Suppose Induction is not true. This means that,
   1.1 Base Case holds: $P(0)$ is true;
   1.2 Induction Step holds: for $\forall n \geq 0$, $P(n) \implies P(n+1)$;
   1.3 But the conclusion doesn't hold, i.e., it isn't the case that ($P(n)$ is true for all non-negative integers).
2. Point (1.3) implies there exists $n \in \mathbb{N}$ s.t., $P(n)$ is false.
3. Now, consider set $S = \{i \in \mathbb{N} \mid P(i) \text{ is false } \}$.

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

1. Suppose Induction is not true. This means that,
   - 1.1 Base Case holds: $P(0)$ is true;
   - 1.2 Induction Step holds: for $\forall n \geq 0$, $P(n) \implies P(n+1)$;
   - 1.3 But the conclusion doesn't hold, i.e., it isn't the case that ($P(n)$ is true for all non-negative integers).
2. Point (1.3) implies there exists $n \in \mathbb{N}$ s.t., $P(n)$ is false.
3. Now, consider set $S = \{i \in \mathbb{N} \mid P(i) \text{ is false } \}$.
4. $S$ is a non-empty (due to 2.) set of non-negative integers, hence by WOP, it has a smallest element, say $i_0 \in S$.

# WOP implies induction

**Theorem: Well-ordering principle implies Induction**

Proof by contradiction:

1. Suppose Induction is not true. This means that,
   1.1 Base Case holds: $P(0)$ is true;
   1.2 Induction Step holds: for $\forall n \geq 0$, $P(n) \implies P(n+1)$;
   1.3 But the conclusion doesn't hold, i.e., it isn't the case that ($P(n)$ is true for all non-negative integers).
2. Point (1.3) implies there exists $n \in \mathbb{N}$ s.t., $P(n)$ is false.
3. Now, consider set $S = \{i \in \mathbb{N} \mid P(i) \text{ is false }\}$.
4. $S$ is a non-empty (due to 2.) set of non-negative integers, hence by WOP, it has a smallest element, say $i_0 \in S$.
5. $i_0 \neq 0$ (due to 1.1) and $i_0 - 1 \notin S$ (since $i_0$ is smallest in $S$).
6. $i_0 - 1 \notin S$ implies $P(i_0 - 1)$ is true (by definition of $S$).
7. By (1.2), $P(i_0)$ must be true, $i_0 \notin S$. Contradiction! $\square$

# The Well Ordering Principle and Induction

## Well Ordering Principle

Every nonempty set of non-negative integers has a smallest element.

## Induction

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

## Theorem: Well-ordering principle iff Induction

# The Well Ordering Principle and Induction

## Well Ordering Principle

Every nonempty set of non-negative integers has a smallest element.

## Induction

Let $P(n)$ be a property of non-negative integers. If

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $P(k) \implies P(k+1)$ (Induction step)

then $P(n)$ is true for all $n \in \mathbb{N}$.

## Theorem: Well-ordering principle iff Induction

So, we could have chosen either one of them as our basic axiom!

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer $> 1$ can be written as a product of primes

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer $> 1$ can be written as a product of primes

Proof by contradiction using WOP!:

- Let $S$ be the set of all integers greater than 1 that cannot be written as a product of primes.

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

**Theorem: Any integer $> 1$ can be written as a product of primes**

Proof by contradiction using WOP!:

- Let $S$ be the set of all integers greater than 1 that cannot be written as a product of primes.
- If $S$ is non-empty, there is a least element in it by WOP.

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

**Theorem:** Any integer $> 1$ can be written as a product of primes

Proof by contradiction using WOP!:

- Let $S$ be the set of all integers greater than 1 that cannot be written as a product of primes.
- If $S$ is non-empty, there is a least element in it by WOP.
- Call this least number $n$. First, $n$ can't be a prime (why?).
- So $n = a \cdot b$, where $n > a, b > 1$.

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

**Theorem:** Any integer $> 1$ can be written as a product of primes

Proof by contradiction using WOP!:

- Let $S$ be the set of all integers greater than 1 that cannot be written as a product of primes.
- If $S$ is non-empty, there is a least element in it by WOP.
- Call this least number $n$. First, $n$ can't be a prime (why?).
- So $n = a \cdot b$, where $n > a, b > 1$.
- Since $a$ and $b$ are smaller than the smallest number in $S$, they can be written as product of primes.
- Let $a = p_1 \ldots p_k$ and $b = q_1 \cdots q_l$. But then $n = p_1 \cdots p_k \cdot q_1 \cdots q_l$, which is a contradiction. □

# Direct application of WOP to prove theorems

– Proving one part of the fundamental theorem of arithmetic.

**Theorem:** Any integer $> 1$ can be written as a product of primes

Proof by contradiction using WOP!:

- Let $S$ be the set of all integers greater than 1 that cannot be written as a product of primes.
- If $S$ is non-empty, there is a least element in it by WOP.
- Call this least number $n$. First, $n$ can't be a prime (why?).
- So $n = a \cdot b$, where $n > a, b > 1$.
- Since $a$ and $b$ are smaller than the smallest number in $S$, they can be written as product of primes.
- Let $a = p_1 \ldots p_k$ and $b = q_1 \cdots q_l$. But then $n = p_1 \cdots p_k \cdot q_1 \cdots q_l$, which is a contradiction. $\square$

Qn: How do you show uniqueness?