CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Aug 08, 2025

Lecture 04 – Induction and Well-Ordering Principle

Recap

Last week

- What are discrete structures?
- Course outline
- Chapter 1: Proofs and structures
  - Propositions: statements that can be assigned a truth value
  - Predicates: propositions with variables
  - Quantifiers
  - Theorems and different types of proofs

Recap

Last week

- What are discrete structures?
- Course outline
- Chapter 1: Proofs and structures
  - Propositions: statements that can be assigned a truth value
  - Predicates: propositions with variables
  - Quantifiers
  - Theorems and different types of proofs

This class

Induction

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$

2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.

3. If 6 is prime, then $6^2 = 30$.
4. x is an even integer iff $x + x^2 - x^3$ is even.

5. There are infinitely many prime numbers.

6. There exist irrational numbers x, y such that x^y is rational.

7. For all integers $n > 1$, $n! < n^n$.
8. There does not exist a program which will always determine whether an arbitrary (input-free) program will halt.

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$
   – By truth tables
2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
   – Direct proof
3. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof
4. x is an even integer iff $x + x^2 - x^3$ is even.
   – Both directions, by contrapositive ($A \to B = \neg B \to \neg A$)
5. There are infinitely many prime numbers.
   – Proof by contradiction
6. There exist irrational numbers x, y such that x^y is rational.
   – Non-constructive proof
7. For all integers $n > 1$, $n! < n^n$.
8. There does not exist a program which will always determine whether an arbitrary (input-free) program will halt.

Types of proofs

1. $\neg(p \wedge q)$ is logically equivalent to $\neg p \vee \neg q$
   – By truth tables
2. For all $a, b, c \in \mathbb{R}^{\geq 0}$, if $a^2 + b^2 = c^2$, then $a + b \geq c$.
   – Direct proof
3. If 6 is prime, then $6^2 = 30$. – Vacuous/trivial proof
4. x is an even integer iff $x + x^2 - x^3$ is even.
   – Both directions, by contrapositive ($A \to B = \neg B \to \neg A$)
5. There are infinitely many prime numbers.
   – Proof by contradiction
6. There exist irrational numbers x, y such that x^y is rational.
   – Non-constructive proof
7. For all integers $n > 1$, $n! < n^n$. – Induction
8. There does not exist a program which will always determine whether an arbitrary (input-free) program will halt.

Induction

Induction (Axiom)

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

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

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

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. □

Where is the bug?

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Proof by induction.

- Base case $n = 1$: $1^3 - 1 = 0$ is div by 6, hence true.

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Proof by induction.

- Base case $n = 1$: $1^3 - 1 = 0$ is div by 6, hence true.
- Induction Hyp Assume $P(k)$: for $k > 0$, $6 \mid k^3 - k$.

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Proof by induction.

- Base case $n = 1$: $1^3 - 1 = 0$ is div by 6, hence true.
- Induction Hyp Assume $P(k)$: for $k > 0$, $6 \mid k^3 - k$.
- To show $P(k+1)$ holds: $6 \mid ((k+1)^3 - (k+1))$.

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Proof by induction.

- Base case $n = 1$: $1^3 - 1 = 0$ is div by 6, hence true.
- Induction Hyp Assume $P(k)$: for $k > 0$, $6 \mid k^3 - k$.
- To show $P(k+1)$ holds: $6 \mid ((k+1)^3 - (k+1))$.

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k) \\ &= (k^3 - k) + 3k(k+1)\end{aligned}$$

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Proof by induction.

- Base case $n = 1$: $1^3 - 1 = 0$ is div by 6, hence true.
- Induction Hyp Assume $P(k)$: for $k > 0$, $6 \mid k^3 - k$.
- To show $P(k+1)$ holds: $6 \mid ((k+1)^3 - (k+1))$.

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k) \\ &= (k^3 - k) + 3k(k+1)\end{aligned}$$

- But $6 \mid (k^3 - k)$ (by induction hyp)

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Proof by induction.

- Base case $n = 1$: $1^3 - 1 = 0$ is div by 6, hence true.
- Induction Hyp Assume $P(k)$: for $k > 0$, $6 \mid k^3 - k$.
- To show $P(k+1)$ holds: $6 \mid ((k+1)^3 - (k+1))$.

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k) \\ &= (k^3 - k) + 3k(k+1)\end{aligned}$$

- But $6 \mid (k^3 - k)$ (by induction hyp)
- $2 \mid k(k+1) \implies 6 \mid 3k(k+1)$

Thus, $6 \mid ((k+1)^3 - (k+1))$.

Exercise!

Prove or disprove: For any positive integer n, $n^3 - n$ is divisible by 6, i.e., $6 \mid (n^3 - n)$.

Proof by induction.

- Base case $n = 1$: $1^3 - 1 = 0$ is div by 6, hence true.
- Induction Hyp Assume $P(k)$: for $k > 0$, $6 \mid k^3 - k$.
- To show $P(k+1)$ holds: $6 \mid ((k+1)^3 - (k+1))$.

$$\begin{aligned}(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= (k^3 - k) + 3(k^2 + k) \\ &= (k^3 - k) + 3k(k+1)\end{aligned}$$

  - But $6 \mid (k^3 - k)$ (by induction hyp)
  - $2 \mid k(k+1) \implies 6 \mid 3k(k+1)$

  Thus, $6 \mid ((k+1)^3 - (k+1))$.
- By Induction we conclude, $\forall n > 0$, $6 \mid n^3 - n$. □

Proving Correctness of Algorithms 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 $f(a, n) = a \cdot f(a, n - 1)$;

Proving Correctness of Algorithms 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 $f(a, n) = a \cdot f(a, n - 1)$;

what does this algorithm do?

Proving Correctness of Algorithms 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 $f(a, n) = a \cdot f(a, n-1)$;

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

Proving Correctness of Algorithms 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 $f(a, n) = a \cdot f(a, n - 1)$;

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

Proof by induction:

- Base case: if $n = 0$, $f(a, 0) = 1 = a^0$ for all non-zero real a.

Proving Correctness of Algorithms 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 $f(a, n) = a \cdot f(a, n - 1)$;

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

Proof by induction:

- Base case: if $n = 0$, $f(a, 0) = 1 = a^0$ for all non-zero real a.
- Induction step: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.

Proving Correctness of Algorithms 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 $f(a, n) = a \cdot f(a, n-1)$;

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

Proof by induction:

- Base case: if $n = 0$, $f(a, 0) = 1 = a^0$ for all non-zero real a.
- Induction step: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.
- Now for $n = k + 1$, $f(a, k+1) = a \cdot f(a, k) = a \cdot a^k = a^{k+1}$ (by Induction Hyp).

Proving Correctness of Algorithms 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 $f(a, n) = a \cdot f(a, n-1)$;

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

Proof by induction:

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

Proving Correctness of Algorithms 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: The above algorithm computes the function $f(a, n) = a^n$ for all non-negative integers n, $a \in \mathbb{R}^{\neq 0}$.

Proof by induction:

- Base case: if $n = 0$, $f(a, 0) = 1 = a^0$ for all non-zero real a.
- Induction step: Assume that for $n = k$, it is true, i.e., $f(a, k) = a^k$.
- Now for $n = k + 1$, $f(a, k+1) = a \cdot f(a, k) = a \cdot a^k = a^{k+1}$ (by Induction Hyp).
- 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 using Induction! (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 using Induction! (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).

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).

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 (one or more) 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 (one or more) 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 (one or more) 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 (one or more) 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 (one or more) 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 (one or more) 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 (one or more) 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 (one or more) 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 (one or more) 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 one or more primes.
- Let $a = p_1 \dots p_k$ and $b = q_1 \cdots q_l$ for $k, l \geq 1$. 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 (one or more) 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 (one or more) 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 one or more primes.
- Let $a = p_1 \dots p_k$ and $b = q_1 \cdots q_l$ for $k, l \geq 1$. But then $n = p_1 \cdots p_k \cdot q_1 \cdots q_l$, which is a contradiction. □

Qn: How do you show uniqueness? (H.W.)

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.
- But now it may be that $p, q \neq k$, so we can't use induction hypothesis.
  - For example, if $k + 1 = 21$, then $21 = 7 \cdot 3$, but $k = 20$, we need $P(7), P(3)$ to hold!

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume induction hypothesis for $n = k$, i.e., $k = p_1 \cdots p_n$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.
- But now it may be that $p, q \neq k$, so we can't use induction hypothesis.
  - For example, if $k + 1 = 21$, then $21 = 7 \cdot 3$, but $k = 20$, we need $P(7), P(3)$ to hold!
- Let us strengthen our induction hypothesis. That is...

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume strong induction hypothesis, i.e., for all $1 \leq r \leq k$, $k = p_1 \cdots p_m$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.

Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

Theorem: Any integer > 1 can be written as a product of one or more primes

Proof by induction:

- Base case: $n = 2$, done.
- Assume strong induction hypothesis, i.e., for all $1 \leq r \leq k$, $k = p_1 \cdots p_m$.
- Consider $n = k + 1$.
- If $k + 1$ is a prime, then done. Else $k + 1 = p \cdot q, p, q > 1$.
- By the stronger hypothesis, we can write $p = p_1 \ldots p_k$ and $q = q_1 \cdots q_l$.
- Therefore $k + 1 = p_1 \cdots p_k \cdot q_1 \cdots q_k$.
- Thus, the statement holds for all $n > 1$. □

Strong Induction

Strong Induction

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

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $(P(0) \wedge P(1) \wedge \cdots \wedge P(k)) \implies P(k+1)$ then $P(n)$ is true for all $n \in \mathbb{N}$. (Induction Step)

Strong Induction

Strong Induction

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

- $P(0)$ is true (Base case)
- for all $k \geq 0$, $(P(0) \wedge P(1) \wedge \cdots \wedge P(k)) \implies P(k+1)$ then $P(n)$ is true for all $n \in \mathbb{N}$. (Induction Step)

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: Strong Induction iff Induction iff WOP

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.
- Base case: n=1.

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.
- Base case: n=1.
- Assume for groups of $2k+1$ students. Now consider a group of $2k+3$ students.

Induction examples

An odd number of students stand at mutually distinct distances. At the same time, each student throws a paper rocket at their nearest neighbour, hitting this person. Use mathematical induction, to show that there is at least one survivor, i.e., at least one student who is not hit by a rocket!

How to show this? What is P(n)?

- $P(n)$ be the statement that there is a survivor whenever $2n+1$ students stand at distinct mutual distances and each student throws a rocket at their nearest neighbour. Show that $P(n)$ is true for all positive integers n.
- Base case: n=1.
- Assume for groups of $2k+1$ students. Now consider a group of $2k+3$ students.
- Consider the closest pair A-B...