# CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Aug 14, 2023

Lecture 04 – Strong Induction, Basic Mathematical Structures

# Logistics

## Exercise Problem Sheets

- Problem sheet 1 released on Friday.
- (Optional) help session to be held this Wednesday at 6.30pm at CC 103 (New CSE/CC building).

# Recap of last three lectures

## Chapter 1: Mathematical reasoning

- Propositions, predicates.
- Axioms, Theorems and Types of proofs: contradiction, contrapositive, etc.
- Principle of Mathematical Induction
- Well-ordering principle.

# 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 $a = p_1 \dots p_k$ 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 $a = p_1 \dots p_k$ 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. □

Qn: How do you show uniqueness?

# Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

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

# Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

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

Proof by induction:

- Base case: $n = 2$, done.
- Assume strong induction hypothesis, i.e., for all $1 \leq r \leq k$, $k = p_1 \cdots p_m$.

# Direct proof by induction

– Proving one part of the fundamental theorem of arithmetic.

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

Proof by induction:

- Base case: $n = 2$, done.
- Assume strong induction hypothesis, i.e., for all $1 \leq r \leq k$, $k = p_1 \cdots p_m$.
- 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 $k \geq 0$, $(P(0) \wedge P(1) \wedge \cdots \wedge P(k)) \implies P(k+1)$ (Induction Step)

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

# Strong Induction

## Strong Induction

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

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

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

## 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

# Another exercise by Strong Induction

## Quotient-Remainder Theorem

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
    3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r$,$0 \leq r < m$.

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
   3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r$, $0 \leq r < m$.
   3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
    3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
    3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on $k'$.

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
   3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on $k'$.
5. By Ind Hyp, $k' = q'm + r'$ for some $q'$, $0 \leq r' < m$.

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
   3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on $k'$.
5. By Ind Hyp, $k' = q'm + r'$ for some $q'$, $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
   - 3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   - 3.2 (to prove): $\exists q^*, r^*$ s.t., $k+1 = q^*m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on $k'$.
5. By Ind Hyp, $k' = q'm + r'$ for some $q'$, $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$
7. Then, $q^*m + r^* = (q'+1)m + r' = q'm + r' + m = k' + m = ((k+1) - m) + m = k + 1$. □

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
   3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on $k'$.
5. By Ind Hyp, $k' = q'm + r'$ for some $q'$, $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$
7. Then, $q^* m + r^* = (q'+1)m + r' = q'm + r' + m = k' + m = ((k+1) - m) + m = k + 1$. □

Qns: Show uniqueness.

# Another exercise by Strong Induction

**Quotient-Remainder Theorem**

For any two $m, n \in \mathbb{N}$, $m \neq 0$, there exists a unique quotient $q$ and remainder $r$ ($q, r \in \mathbb{N}$), such that

$$n = q \cdot m + r, \quad 0 \leq r < m$$

1. Fix any $m > 0$, we use strong induction on $n$.
2. Base cases: $n \in \{0, \ldots, m-1\}$. What should $q$ and $r$ be?
3. Induction step: We prove for all $k \geq m$,
   3.1 (ind hyp): if $\forall n \in \mathbb{N}$, $n \leq k$, $\exists q, r$ s.t. $n = qm + r, 0 \leq r < m$.
   3.2 (to prove): $\exists q^*, r^*$ s.t., $k + 1 = q^* m + r^*$ for $0 \leq r^* < m$.
4. Take $k' = (k+1) - m = k - (m-1) \leq k$. i.e., $k' \leq k$, so we can apply ind hyp on $k'$.
5. By Ind Hyp, $k' = q'm + r'$ for some $q'$, $0 \leq r' < m$.
6. Now to prove 3.2, we choose $q^* = q' + 1, r^* = r'$
7. Then, $q^* m + r^* = (q'+1)m + r' = q'm + r' + m = k' + m = ((k+1) - m) + m = k + 1$. □

Qns: Show uniqueness. Also, what if $m, n \in \mathbb{Z}, m \neq 0$?

# From proofs to structures

# From proofs to structures

**Next: Chapter 2: Basic Mathematical Structures**

- Finite and infinite sets, Functions
- Relations