# Overview of the Related Concepts

Ebru Aydin Gol

CENG 280, 2022

Finite and infinite sets

Three fundamental proof techniques

Closures

# Finite and Infinite Sets

**Set:** collection of objects
**Equinumerous:** Sets $A$ and $B$ are equinumerous if there exists a bijection $f : A \to B$ (one-to-one and onto)
**Finite:** A set is finite if it is equinumerous with $\{1, \ldots, n\}$ for some natural number $n$.
**Infinite:** A set is infinite if it is not finite. E.g. natural numbers, the set of integers, set of real numbers, etc.
**Countably infinite:** A set is countably infinite if it is equinumerous with $\mathbb{N}$ (natural numbers).
**Uncountable:** A set is uncountable, if it is not countable.
*An alphabet is a finite set of symbols.*
*A finite sequence of symbols from an alphabet is a string.*
*The set of all strings over an alphabet $\Sigma$ is denoted by $\Sigma^\star$*
*A subset $L$ of $\Sigma^\star$ is a language.*

To show that a set $A$ is countably infinite, define a bijection between $A$ and $\mathbb{N}$. Enumerate set $A = \{a_0, a_1, \ldots, \}$, $f : N \rightarrow A$, $f(i) = a_i$.

### Example

Show that the following sets are countable.

- Union two countably infinite sets.
- Union of countably infinite collection of countably infinite sets ($\mathbb{N} \times \mathbb{N}$).

# Finite / countably infinite / uncountably infinite

Consider alphabet $\Sigma = \{0, 1\}$. Decide whether the following sets are finite/countably infinite / uncountably infinite

- $\Sigma^\star$
- $L$ such that $L \subseteq \Sigma^\star$
- $\{L \mid L \subseteq \Sigma^\star\}$

Consider alphabet $\Sigma = \{\}$. Decide whether the following sets are finite/countably infinite / uncountably infinite

- $\Sigma^\star$
- $\{L \mid L \subseteq \Sigma^\star\}$

# Three Fundamental Proof Techniques

The principle of mathematical induction.
The pigeon hole principle.
The diagonalization principle.

# Three Fundamental Proof Techniques

## The principle of mathematical induction

Let $A$ be a set of natural numbers such that

$0 \in A$.

For each $n \in \mathbb{N}$, if $\{0, 1, \ldots, n\} \subseteq A$, then $n + 1 \in A$.

Then $A = \mathbb{N}$. (*Prove it by contradiction.*)

The goal is to prove that "For all natural numbers $n \in \mathbb{N}$, property $P$ is true". The MI principle is applied to the set $A = \{n \mid P \text{ is true for } n\}$.

# Three Fundamental Proof Techniques

The goal is to prove that "For all natural numbers $n \in \mathbb{N}$, property $P$ is true". The MI principle is applied to the set $A = \{n \mid P \text{ is true for } n\}$.

**Basis step:** Show that $P$ is true for 0. $(0 \in A)$
**Induction hypothesis:** For an arbitrary $n \in \mathbb{N}$, assume that $P$ holds for each $\{0, \dots, n\}$. $(\{0, 1, \dots, n\} \subseteq A)$
**Induction:** Show that $P$ is true for $n + 1$. $(n + 1 \in A)$

Then, by induction principle, $A = \mathbb{N}$, thus, $P$ is true for any $n \in \mathbb{N}$.

# Three Fundamental Proof Techniques

**The pigeonhole principle**

If $A$ and $B$ are finite sets with $|A| > |B|$, then there is no one-to-one function from $A$ to $B$.

Proof by MI on $n = |B|$.

**Binary relation:** $A \neq \emptyset$, $R \subseteq A \times A$ is a binary relation on $A$.
A path of length $n \geq 1$ in the relation is a finite sequence $(a_1, \dots, a_n)$ such that $(a_i, a_{i+1}) \in R$ for $i = 1, \dots, n-1$. $(a_1, \dots, a_n)$ is a cycle if all $a_i$ are distinct and $(a_n, a_1) \in R$.

**Theorem**

*Let $R$ be a binary relation on a finite set $A$. If there is a path from $a$ to $b$ in $R$, then there is a path of length at most $|A|$.*

Proof by contradiction and Pigeonhole principle.

# Three Fundamental Proof Techniques

## The diagonalization principle

Let $R$ be a binary relation on a set $A$, and let the diagonal set $D$ for $R$ be defined as $D = \{a \mid a \in A \text{ and } (a, a) \notin R\}$. For each $a \in A$, let $R_a = \{b \mid b \in A \text{ and } (a, b) \in R\}$. Then $D$ is distinct from each $R_a$.

The diagonalization principle is used to prove that a set is uncountable.
*The idea:* for any enumeration, there exists an element that was not in the list.

## Theorem

*The set* $2^{\mathbb{N}}$ *is uncountable.*

Proof by diagonalization principle.

# Closures and Algorithms

## Definition (reflexive transitive closure)

Let $R$ be a binary relation on $A$. $R^\star$ is called the reflexive, transitive closure of $R$ if

- $R \subseteq R^\star$
- $R^\star$ is reflexive and transitive
- $R^\star$ is the smallest set with these properties.

## Definition (reflexive transitive closure)

Let $R$ be a binary relation on $A$. The reflexive transitive closure of $R$ is the relation:

$$R^\star = \{(a, b) \in A \times A \mid \text{ there is a path from } a \text{ to } b \text{ in } R\}$$

# Closures and Algorithms

## Definition (reflexive transitive closure)

Let $R$ be a binary relation on $A$. The reflexive transitive closure of $R$ is the relation:

$$R^\star = \{(a, b) \in A \times A \mid \text{ there is a path from } a \text{ to } b \text{ in } R\}$$

**Initially** $R^\star = \{\}$
**for** $i = 1, \ldots, |A|$
  **for each** $(b_1, \ldots, b_i) \in A^i$ **do**
    **if** $b_1, \ldots, b_i$ is a path in $R$, then add $(b_1, b_i)$ to $R^\star$

# Closures and Algorithms

## Definition (closure)

Let $D$ be a set, let $n \geq 0$, and let $R \subseteq D^{n+1}$ be a $(n+1)$-ary relation on $D$. Then a subset $B$ of $D$ is said to be **closed under** $R$ if $b_{n+1} \in B$ whenever

$b_1, \ldots, b_n \in B$ and

$(b_1, \ldots, b_n, b_{n+1}) \in R$

Any property of the form "the set $B$ is closed under relations $R_1, \ldots, R_m$" is called a closure property of $B$.

# Closures and Algorithms

For a set $A$, the set $S$ satisfies the **inclusion property associated with** $A$ if $A \subseteq S$. Any inclusion property is a closure property by taking $R$ to be unary relation $\{(a) \mid a \in A\}$.

Relations are sets, so we can state one relation is closed under another.

**Transitivity is a closure property:** Let $D$ be a set. $R \subseteq D \times D$ be a binary relation. TP: if $(a, b), (b, c) \in R$, then $(a, c) \in R$.
$Q = \{((a, b), (b, c), (a, c)) \mid a, b, c \in D\}$. $R$ is closed under $Q$ iff $R$ is transitive.

**Reflexivity is a closure property:** Let $D \neq \emptyset$. $Q' = \{(a, a) \mid a \in D\}$. $R$ is closed under $Q'$ iff $R$ is reflexive (inclusion property).

# Closures and Algorithms

**Theorem**

*Let $P$ be a closure property defined by relations $R_1, \ldots, R_m$ on a set $D$. Let $A \subseteq D$. Then there exists a unique set $B$ such that $A \subseteq B$ and $B$ has property $P$.*

**N** is the closure under addition of the set $\{0, 1\}$. **N** is closed under addition and multiplication, but not subtraction.