cse303
ELEMENTS OF THE THEORY OF COMPUTATION

Professor Anita Wasilewska
CHAPTER 1
SETS, RELATIONS, and LANGUAGES

1. Sets
2. Relations and Functions
3. Special types of binary relations
4. Finite and Infinite Sets
5. Fundamental Proof Techniques
6. Closures and Algorithms
7. Alphabets and languages
8. Finite Representation of Languages
CHAPTER 1

PART 4: Finite and Infinite Sets
Equinumerous Sets

Equinumerous sets
We call two sets $A$ and $B$ are equinumerous if and only if there is a bijection function $f : A \rightarrow B$, i.e. there is $f$ is such that

$$f : A \xrightarrow{1-1, onto} B$$

Notation
We write $A \sim B$ to denote that the sets $A$ and $B$ are equinumerous and write symbolically

$$A \sim B \text{ if and only if } f : A \xrightarrow{1-1, onto} B$$
Equinumerous Relation

**Observe** that for any set $X$, the relation $\sim$ is an equivalence on the set $2^X$, i.e.

$$\sim \subseteq 2^X \times 2^X$$

is reflexive, symmetric and transitive and for any set $A$ the equivalence class

$$[A] = \{ B \in 2^X : A \sim B \}$$

describes for finite sets all sets that have the same number of elements as the set $A$
Equinumerous Relation

**Observe** also that the relation $\sim$ when considered for any sets $A, B$ is not an equivalence relation as its **domain** would have to be the set of all sets that does not exist.

We extend the notion of "the same number of elements" to **any** sets by introducing the notion of **cardinality** of sets.
Cardinality of Sets

Cardinality definition
We say that $A$ and $B$ have the same cardinality if and only if they are equipotent, i.e.

$$A \sim B$$

Cardinality notations
If sets $A$ and $B$ have the same cardinality we denote it as:

$$|A| = |B| \text{ or } \text{card}A = \text{card}B$$
Cardinality of Sets

Cardinality

We put the above together in one definition

\(|A| = |B|\) if and only if

there is a function \(f\) is such that

\[ f : A \xrightarrow{1-1,\text{onto}} B \]
Finite and Infinite Sets

Definition
A set $A$ is **finite** if and only if there is $n \in N$ and there is a function

$$f : \{0, 1, 2, ..., n - 1\} \rightarrow A$$

In this case we have that

$$|A| = n$$

and say that the set $A$ has $n$ elements
Finite and Infinite Sets

Definition
A set $A$ is infinite if and only if $A$ is not finite

Here is a theorem that characterizes infinite sets

Dedekind Theorem
A set $A$ is infinite if and only if there is a proper subset $B$ of the set $A$ such that

$$|A| = |B|$$
Infinite Sets Examples

E1 Set $\mathbb{N}$ of natural numbers is infinite

Consider a function $f$ given by a formula

$$f(n) = 2n \text{ for all } n \in \mathbb{N}$$

Obviously

$$f : \mathbb{N} \xrightarrow{1-1,onto} 2\mathbb{N}$$

By Dedekind Theorem the set $\mathbb{N}$ is infinite as the set $2\mathbb{N}$ of even numbers are a proper subset of natural numbers $\mathbb{N}$
Infinite Sets Examples

\bf{E2} Set \( R \) of real numbers is infinite

Consider a function \( f \) given by a formula 
\[ f(x) = 2^x \] for all \( x \in R \)

Obviously

\[ f : R \xrightarrow{1-1,onto} R^+ \]

By Dedekind Theorem the set \( R \) is infinite as the set \( R^+ \) of positive real numbers are a proper subset of real numbers \( R \)
**Countably Infinite Sets**

**Cardinal Number** $\aleph_0$

**Definition**

A set $A$ is called **countably infinite** if and only if it has the same **cardinality** as the set $N$ natural numbers, i.e. when

$$|A| = |N|$$

The **cardinality** of natural numbers $N$ is called $\aleph_0$ (Aleph zero) and we write

$$|N| = \aleph_0$$
Definition
For any set $A$,

$$|A| = \aleph_0 \quad \text{if and only if} \quad |A| = |\mathbb{N}|$$

Directly from definitions we get the following

Fact 1
A set $A$ is countably infinite if and only if $|A| = \aleph_0$
Countably Infinite Sets

Fact 2
A set $A$ is **countably infinite** if and only if all elements of $A$ can be put in a 1-1 sequence.

Other name for **countably infinite** set is **infinitely countable** set and we will use both names.
Countably Infinite Sets

In a case of an infinite set $A$ and not 1-1 sequence we can ”prune” all repetitive elements to get a 1-1 sequence, i.e. we prove the following

**Fact 2a**

An infinite set $A$ is **countably infinite** if and only if all elements of $A$ can be put in a sequence
Countable and Uncountable Sets

Definition
A set $A$ is **countable** if and only if $A$ is finite
or countably infinite

Fact 3
A set $A$ is **countable** if and only if $A$ is finite
or $|A| = \aleph_0$, i.e. $|A| = |N|$
Countable and Uncountable Sets

Definition
A set $A$ is **uncountable** if and only if $A$ is not countable

Fact 4
A set $A$ is **uncountable** if and only if $A$ is infinite and $|A| \neq \aleph_0$, i.e. $|A| \neq |N|$

Fact 5
A set $A$ is **uncountable** if and only if its elements **can not** be put into a sequence

Proof proof follows directly from definition and Facts 2, 4
Countably Infinite Sets

We have proved the following

Fact 2a
An infinite set $A$ is **countably infinite** if and only if all elements of $A$ can be put in a sequence

We use it now to prove two **theorems** about **countably infinite** sets
Countably Infinite Sets

Union Theorem
Union of two countably infinite sets is a countably infinite set

Proof
Let $A$, $B$ be two disjoint infinitely countable sets
By Fact 2 we can list their elements as 1-1 sequences

\[ A : \ a_0, a_1, a_2, \ldots \ \text{and} \ \ B : \ b_0, b_1, b_2, \ldots \]

and their union can be listed as 1-1 sequence

\[ A \cup B : \ a_0, b_0, a_1, b_1, a_2, b_2, \ldots, \ldots \]

In a case not disjoint sets we proceed the same and then "prune" all repetitive elements to get a 1-1 sequence
Countably Infinite Sets

Product Theorem
Cartesian Product of two countably infinite sets is a countably infinite set

Proof
Let \( A, B \) be two infinitely countable sets
By Fact 2 we can list their elements as 1-1 sequences

\[
A : \quad a_0, a_1, a_2, \ldots \quad \text{and} \quad B : \quad b_0, b_1, b_2, \ldots
\]

We list their Cartesian Product \( A \times B \) as an infinite table
\[
(a_0, b_0), (a_0, b_1), (a_0, b_2), (a_0, b_3), \ldots \\
(a_1, b_0), (a_1, b_1), (a_1, b_2), (a_1, b_3), \ldots \\
(a_2, b_0), (a_2, b_1), (a_2, b_2), (a_2, b_3), \ldots \\
(a_3, b_0), (a_3, b_1), (a_3, b_2), (a_3, b_3), \ldots \\
\ldots, \ldots, \ldots, \ldots, \ldots, \ldots, \ldots,
Cartesian Product Theorem Proof

Observe that even if the table is infinite each of its diagonals is finite

\[(a_0, b_0), (a_0, b_1), (a_0, b_2), (a_0, b_3), (a_0, b_4), \ldots, \ldots\]
\[(a_1, b_0), (a_1, b_1), (a_1, b_2), (a_1, b_3), \ldots\]
\[(a_2, b_0), (a_2, b_1), (a_2, b_2), (a_2, b_3), \ldots\]
\[(a_3, b_0), (a_3, b_1), (a_3, b_2), (a_3, b_3), \ldots\]
\[\ldots, \ldots, \ldots, \ldots, \ldots,\]

We list now elements of \( A \times B \) one diagonal after the other. Each diagonal is finite, so now we know when one finishes and other starts.
Cartesian Product Theorem Proof

\( A \times B \) becomes now the following sequence

\[
(a_0, b_0),
(a_1, b_0), (a_0, b_1),
(a_2, b_0), (a_1, b_1), (a_0, b_2),
(a_3, b_0), (a_2, b_1), (a_1, b_2), (a_0, b_3),
(a_3, b_1), (a_2, b_2), (a_1, b_3), (a_0, b_4), \ldots,
\ldots, \ldots, \ldots, \ldots,
\]

We prove by **Mathematical induction** that the sequence is **well defined** for all \( n \in N \) and hence that \( |A \times B| = |N| \)

It **ends** the proof of the **Product Theorem**
Union and Cartesian Product Theorems

Observe that the both Union and Product Theorems can be generalized by Mathematical Induction to the case of Union or Cartesian Products of any finite number of sets.
Uncountable Sets

Theorem 1
The set $R$ of real numbers is uncountable

Proof
We first prove (homework problem 1.5.11) the following

Lemma 1
The set of all real numbers in the interval $[0,1]$ is uncountable

Then we use the Lemma 2 below (to be proved it as an exercise) and the fact that $[0,1] \subseteq R$ and this ends the proof

Lemma 2 For any sets $A,B$ such that $B \subseteq A$ and $B$ is uncountable we have that also the set $A$ is uncountable
Special Uncountable Sets

Cardinal Number $C$ - Continuum
We denote by $C$ the cardinality of the set $R$ of real numbers $C$ is a new **cardinal number** called **continuum** and we write

$$|R| = C$$

**Definition**
We say that a set $A$ has **cardinality** $C$ (continuum) if and only if

$$|A| = |R|$$

We write it

$$|A| = C$$
Sets of Cardinality $\mathcal{C}$

Example

The set of positive real numbers $\mathbb{R}^+$ has cardinality $\mathcal{C}$ because a function $f$ given by the formula

$$f(x) = 2^x \text{ for all } x \in \mathbb{R}$$

is 1-1 function and maps $\mathbb{R}$ onto the set $\mathbb{R}^+$
Sets of Cardinality $C$

**Theorem 2**
The set $2^\mathbb{N}$ of all subsets of natural numbers is *uncountable*

**Proof**
in the book p.28

**Theorem 3**
The set $2^\mathbb{N}$ has cardinality $C$, i.e.

$$|2^\mathbb{N}| = C$$

**Proof**
The proof of this theorem is not trivial and is not in the scope of this course
Cantor Theorem

Cantor Theorem (1891)
For any set $A$,

$$|A| < |2^A|$$

where we define

$|A| \leq |B|$ if and only if $A \sim C$ and $C \subseteq B$

$|A| < |B|$ if and only if $|A| \leq |B|$ and $|A| \neq |B|$
Cantor Theorem

Directly from the definition we have the following

**Fact 6**
If $A \subseteq B$ then $|A| \leq |B|$

We know that $|\mathbb{N}| = \aleph_0$, $C = |\mathbb{R}|$, and $\mathbb{N} \subseteq \mathbb{R}$ hence from Fact 6, $\aleph_0 \leq C$, but $\aleph_0 \neq C$, as the set $\mathbb{N}$ is countable and the set $\mathbb{R}$ is uncountable

Hence we proved

**Fact 7**

$\aleph_0 < C$
Uncountable Sets of Cardinality Greater than $\mathcal{C}$

By **Cantor Theorem** we have that

$$|N| < |\mathcal{P}(N)| < |\mathcal{P}(\mathcal{P}(N))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(N)))| < \ldots$$

All sets

$$\mathcal{P}(\mathcal{P}(N)), \mathcal{P}(\mathcal{P}(\mathcal{P}(N))) \ldots$$

are **uncountable** with **cardinality greater** than $\mathcal{C}$, as by Theorem 3, Fact 7, and **Cantor Theorem** we have that

$$\aleph_0 < \mathcal{C} < |\mathcal{P}(\mathcal{P}(N))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(N)))| < \ldots$$
Countable and Uncountable Sets

Here are some basic **Theorem** and **Facts**

**Union 1**
Union of two infinitely countable (of cardinality $\aleph_0$) sets is an infinitely countable set
This means that
$$\aleph_0 + \aleph_0 = \aleph_0$$

**Union 2**
Union of a finite (of cardinality $n$) set and infinitely countable (of cardinality $\aleph_0$) set is an infinitely countable set
This means that
$$\aleph_0 + n = \aleph_0$$
Countable and Uncountable Sets

**Union 3**

Union of an infinitely countable (of cardinality \( \aleph_0 \)) set and a set of the same cardinality as real numbers i.e. of the cardinality \( C \) has the same cardinality as the set of real numbers.

This means that

\[
\aleph_0 + C = C
\]

**Union 4**

Union of two sets of cardinality the same as real numbers (of cardinality \( C \)) has the same cardinality as the set of real numbers.

This means that

\[
C + C = C
\]
Countable and Uncountable Sets

Product 1
Cartesian Product of two infinitely countable sets is an infinitely countable set

\[ \aleph_0 \cdot \aleph_0 = \aleph_0 \]

Product 2
Cartesian Product of a non-empty finite set and an infinitely countable set is an infinitely countable set

\[ n \cdot \aleph_0 = \aleph_0 \quad \text{for} \quad n > 0 \]
Countable and Uncountable Sets

**Product 3**
Cartesian Product of an *infinitely countable* set and an *uncountable* set of cardinality $C$ has the cardinality $C$

$$\aleph_0 \cdot C = C$$

**Product 4**
Cartesian Product of two *uncountable* sets of cardinality $C$ has the cardinality $C$

$$C \cdot C = C$$
Countable and Uncountable Sets

Power 1
The set $2^\mathbb{N}$ of all subsets of natural numbers (or of any countably infinite set) is uncountable set of cardinality $\mathcal{C}$, i.e. has the same cardinality as the set of real numbers

$$2^{\aleph_0} = \mathcal{C}$$

Power 2
There are $\mathcal{C}$ of all functions that map $\mathbb{N}$ into $\mathbb{N}$

Power 3
There are $\mathcal{C}$ possible sequences that can be form out of an infinitely countable set

$$\aleph_0^{\aleph_0} = \mathcal{C}$$
Countable and Uncountable Sets

Power 4
The set of all functions that map $\mathbb{R}$ into $\mathbb{R}$ has the cardinality $\mathcal{C}^\mathcal{C}$.

Power 5
The set of all real functions of one variable has the same cardinality as the set of all subsets of real numbers

$$\mathcal{C}^\mathcal{C} = 2^\mathcal{C}$$
Countable and Uncountable Sets

Theorem 4

\[ n < \aleph_0 < C \]

Theorem 5

For any non empty, finite set \( A \), the set \( A^* \) of all finite sequences formed out of \( A \) is countably infinite, i.e.

\[ |A^*| = \aleph_0 \]

We write it as

If \( |A| = n, \ n \geq 1 \), then \( |A^*| = \aleph_0 \)
Simple Short Questions

Q1 Set $A$ is uncountable iff $A \subseteq \mathbb{R}$ ($\mathbb{R}$ is the set of real numbers)

Q2 Set $A$ is countable iff $N \subseteq A$ where $N$ is the set of natural numbers

Q3 The set $\mathbb{2}^N$ is infinitely countable

Q4 The set $A = \{\{n\} \in 2^N : n^2 + 1 \leq 15\}$ is infinite

Q5 The set $A = \{(\{n\}, n) \in 2^N \times N : 1 \leq n \leq n^2\}$ is infinitely countable

Q6 Union of an infinite set and a finite set is an infinitely countable set
Answers to Simple Short Questions

Q1 Set \( A \) is uncountable if and only if \( A \subseteq R \) (\( R \) is the set of real numbers)

No

The set \( 2^R \) is uncountable, as \( |R| < |2^R| \) by Cantor Theorem, but \( 2^R \) is not a subset of \( R \)

Also for example, \( N \subseteq R \) and \( N \) is not uncountable
Q2 Set $A$ is countable if and only if $N \subseteq A$, where $N$ is the set of natural numbers.

NO

For example, the set $A = \{\emptyset\}$ is countable as it is finite, but $N \notin \{\emptyset\}$

In fact, $A$ can be any finite set or any $A$ can be any infinite set that does not include $N$, for example,

$$A = \{\{n\} : n \in N\}$$
Answers to Simple Short Questions

Q3  The set $2^N$ is infinitely countable
    NO
    $|2^N| = |R| = C$ and hence $2^N$ is uncountable

Q4  The set $A = \{ \{n\} \in 2^N : n^2 + 1 \leq 15 \}$ is infinite
    NO
    The set $\{ n \in N : n^2 + 1 \leq 15 \} = \{0, 1, 2, 3\}$,
    Hence the set $A = \{ \{0\}, \{1\}, \{2\}, \{3\} \}$ is finite
Q5  The set $A = \{(\{n\}, n) \in 2^N \times N : 1 \leq n \leq n^2\}$ is \textbf{infinitely countable} (countably infinite).

\textbf{YES}

Observe that the condition $n \leq n^2$ holds for all $n \in N$, so the set $B = \{n : n \leq n^2\}$ is \textbf{infinitely countable}.

The set $C = \{(\{n\} \in 2^N : 1 \leq n \leq n^2\}$ is also \textbf{infinitely countable} as the function given by a formula $f(n) = \{n\}$ is $1-1$ and maps $B$ onto $C$, i.e. $|B| = |C|$

The set $A = C \times B$ is hence \textbf{infinitely countable} as the Cartesian Product of two \textbf{infinitely countable} sets.
CHAPTER 1

PART 5: Fundamental Proof Techniques

1. Counting Functions Theorem
2. The Pigeonhole Principle
3. The Diagonalization Principle
Mathematical Induction Examples

Counting Functions Theorem

For any finite, non empty sets $A$, $B$, there are

$$|B|^{|A|}$$

functions that map $A$ into $B$

Proof

We conduct the proof by Mathematical Induction over the number of elements of the set $A$, i.e. over $n \in N - \{0\}$, where $n = |A|$
Counting Functions Theorem Proof

Base case $n = 1$
We have hence that $|A| = 1$ and let $|B| = m, \ m \geq 1$, i.e.

$$A = \{a\} \text{ and } B = \{b_1, \ldots, b_m\}, \ m \geq 1$$

We have to prove that there are

$$|B|^{|A|} = m^1$$

functions that map $A$ into $B$

The base case holds as there are exactly $m^1 = m$ functions $f: \{a\} \rightarrow \{b_1, \ldots, b_m\}$ defined as follows

$$f_1(a) = b_1, \ f_2(a) = b_2, \ \ldots, \ f_m(a) = b_m$$
Inductive Step
Let \( A = A_1 \cup \{a\} \) for \( a \notin A_1 \) and \( |A_1| = n \)
By inductive assumption, there are \( m^n \) functions
\[
f : A \longrightarrow B = \{b_1, \ldots, b_m\}
\]
We group all functions that map \( A_1 \) into \( B \) in the following groups.
Group 1 contains all functions \( f_1 \) such that
\[
f_1 : A \longrightarrow B
\]
and they have the following property
\[
f_1(a) = b_1, \quad f_1(x) = f(x) \quad \text{for all} \quad f : A \longrightarrow B \quad \text{and} \quad x \in A_1
\]
By inductive assumption there are \( m^n \) functions in the Group 1
Inductive Step

**Group i**  We define now Group $i$, for $1 \leq i \leq m$, where $m = |B|$ as follows

Each Group $i$ contains all functions $f_i$ such that

$$f_i: A \rightarrow B$$

and they have the following property

$$f_i(a) = b_1, \quad f_i(x) = f(x) \quad \text{for all} \quad f: A \rightarrow B \quad \text{and} \quad x \in A_1$$

By inductive assumption there are $m^n$ functions in each of the Group $i$

**Observe** that there are $m = |B|$ groups and each of them has $m^n$ elements, so all together there are

$$m(m^n) = m^{n+1}$$

functions, what ends the proof
Mathematical Induction Examples

We now use Mathematical Induction to prove our other fundamental proof technique: the pigeonhole principle.

**Pigeonhole Principle Theorem**

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

**Proof** by Mathematical Induction over $n = |B|$

**Base case** $n = 0$

Assume $|B| = 0$, that is, $B = \emptyset$. Then there is no function $f : A \rightarrow B$ whatsoever; let alone a one-to-one function.
Pigeonhole Principle Theorem Proof

**Inductive Assumption**

Any function \( f : A \rightarrow B \) is not one-to one provided \(|A| > |B|\), and \(|B| \leq n, \ n \geq 0\)

**Inductive Step**

Suppose that \( f : A \rightarrow B \), \(|A| > |B|\), and \(|B| = n + 1\)

We have to show that \( f \) is not one-to one under the Inductive Assumption

Choose some element \( a \in A \). Since \(|A| > |B|\), and \(|B| = n + 1 \geq 1\) such choice is possible

Observe now that if there is another element \( a' \in A \) such that \( f(a) = f(a') \), then obviously \( f \) is not one-to one and we are done
So, suppose now that \( a \) is the only element mapped by \( f \) to \( f(a) \)
Consider then the sets \( A - \{a\} \) and \( B - \{f(a)\} \) and a function

\[
g : A - \{a\} \longrightarrow B - \{f(a)\}
\]
such that

\[
g(x) = f(x) \quad \text{for all } x \in A
\]
Observe that the Inductive Assumption applies to \( g \) because

\[
|B - \{f(a)\}| = n \quad \text{and} \quad |A - \{a\}| = |A| - 1 > |B| - 1 = |B - \{f(a)\}|
\]
Therefore the function \( g \) is not one-to one and as \( g(x) = f(x) \) for all \( x \in A \) we have that also \( f \) is not one-to one
By Mathematical Induction there is no one-to one function from \( A \) to \( B \)
Pigeonhole Principle Theorem Application

The Pigeonhole Principle Theorem is a quite simple fact but is used in a large variety of proofs including many in this course. We present here just one simple application which we will use in later Chapters.

**Definition**

Let $A \neq \emptyset$ and $R \subseteq A \times A$ be a binary relation in the set $A$. A **path** in the binary relation $R$ is a finite sequence $a_1, \ldots, a_n$ such that $(a_i, a_{i+1}) \in R$, for $i = 1, 2, \ldots, n - 1$ and $n \geq 1$.

The path $a_1, \ldots, a_n$ is said to be from $a_1$ to $a_n$. The **length** of the path $a_1, \ldots, a_n$ is $n$. The path $a_1, \ldots, a_n$ is a **cycle** if $a_i$ are all distinct and also $(a_n, a_1) \in R$. 
Path Theorem
Let $R$ be a binary relation on a finite set $A$ and let $a, b \in A$.

If there is a path from $a$ to $b$ in $R$,

Then there is a path of length at most $|A|$.

Proof
Suppose that $a_1, \ldots, a_n$ is the shortest path from $a = a_1$ to $b = a_n$, that is, the path with the smallest length, and suppose that $n > |A|$. By Pigeonhole Principle Theorem there is an element in $A$ that repeats on the path, say $a_i = a_j$ for some $1 \leq i < j \leq n$.

But then $a_1, \ldots, a_i, a_{j+1}, \ldots, a_n$ is a shorter path from $a$ to $b$, contradicting $a_1, \ldots, a_n$ being the shortest path.
The Diagonalization Principle

Here is yet another Theorem which justifies a new proof technique

Diagonalization Principle Theorem

Let \( R \) be a binary relation on a set \( A \) and let \( D \), the diagonal set for \( R \) be as follows

\[
D = \{ a \in A : (a, a) \notin R \}
\]

For each \( a \in A \), let

\[
R_a = \{ b \in A : (a, b) \in R \}
\]

Then \( D \) is distinct from each \( R_a \)
The Diagonalization Principle Applications

The most "classic" applications are the following

**Cantor Theorem 2 (Georg Cantor 1845-1918)**

Let \( N \) be the set on natural numbers

\[ 2^N \text{ is uncountable} \]

**Proof** in the Book on page 28

**Real Numbers Theorem**

The set of real numbers in the interval \([0, 1]\) is uncountable

**Proof** This is your homework problem and I will do the proof in class