cse303
ELEMENTS OF THE THEORY OF COMPUTATION

Professor Anita Wasilewska
LECTURE 2
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 iff there is a bijection function $f : A \rightarrow B$, i.e. $f$ is such that $f : A \overset{1-1,onto}{\rightarrow} B$

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

$$A \sim B \text{ iff } f : A \overset{1-1,onto}{\rightarrow} B$$
Equinumerous Relation

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

$\sim \subseteq 2^X \times 2^X$ is reflexive, symmetric and transitive and 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 $A$ (f is bijection)

**Observe** that $\sim$ is defined for any sets $A, B$, but in not an equivalence relation for any $A,B$ 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 iff they are equipotent, i.e. \( A \sim B \)

Cardinality notations
If sets \( A \) and \( B \) have the same cardinality we denote it as:
\[
|A| = |B| \quad \text{or} \quad \text{card}A = \text{card}B \quad \text{or} \quad A \sim B
\]

Cardinality We put the above notations together in one definition:
\[
|A| = |B| \quad \text{(this is the notation we will use)} \quad \text{iff} \quad \text{there is a function } f \text{ is such that}
\]
\[
f : A \xrightarrow{\text{1-1,onto}} B
\]
Finite and Infinite Sets

**Definition**  A set $A$ is finite iff there is $n \in \mathbb{N}$ and a function $f : \{0, 1, 2, ..., n - 1\} \rightarrow A$ that is $1-1$ and onto.

In this case we have that $|A| = n$

and say that the set $A$ has $n$ elements, i.e.

**Definition**  A set $A$ is infinite iff $A$ is NOT finite

Here is a theorem that characterizes infinite sets

**Dedekind Theorem**

A set $A$ is infinite iff there is a proper subset $B$ of the set $A$ such that $|A| = |B|$ i.e. when for a certain proper subset $B$ of $A$ we have that $A \sim B$
Infinite Sets Examples

**E1  Set N of natural numbers is infinite**
Consider a function \( f \) given by a formula \( f(n) = 2n \) for all \( n \in N \). Obviously
\[
f : N \xrightarrow{1-1, \text{onto}} 2N
\]
By **Dedekind Theorem** the set \( N \) is infinite as the set \( 2N \) of even numbers are a proper subset of natural numbers \( N \)

**E2  Set R of real numbers is infinite**
Consider a function \( f \) given by a formula \( f(x) = x^2 \) for all \( x \in R \). Obviously
\[
f : R \xrightarrow{1-1, \text{onto}} R^+
\]
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 it has the same cardinality as the set natural numbers $N$, i.e. when $|A| = |N|$

The cardinality of natural numbers $N$ is called $\aleph_0$ (Aleph zero)

We write $|N| = \aleph_0$

Definition
For any set $A$,

$$|A| = \aleph_0 \quad \text{iff} \quad A \sim N \quad \text{i.e.} \quad |A| = |N|$$

Directly from definitions we get that

**Fact 1** A set $A$ is countably infinite if $|A| = \aleph_0$

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

**Other name** for countably infinite set is infinitely countable set
Countable and Uncountable Sets

Definition A set $A$ is **countable** iff $A$ is finite or countably infinite.

Fact 3 A set $A$ is **countable** iff $A$ is finite or $|A| = \aleph_0$.

Definition A set $A$ is **uncountable** iff $A$ is not countable.

Fact 4 A set $A$ is **uncountable** iff $A$ is infinite and $|A| \neq \aleph_0$.

Directly from definition and Facts 2, 3 we get

Fact 5 A set $A$ is **uncountable** iff its elements can’t be put into a 1-1 sequence.
Uncountable Sets

We use is Fact 5 to prove

**Theorem 1**    The set \( R \) of real numbers is uncountable

**Proof**    We first prove (next lecture and homework problem 1.5.11) that

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

Then we use the following Lemma 2 below (to be proved it as an exercise!) and the fact that \([0,1] \subseteq R\) and get the proof of Theorem 1

**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
Definition \( C \) (continuum) is a cardinality of the set of real numbers \( R \), i.e. \( C = |R| \)

Definition
A set \( A \) has a cardinality \( C \), i.e. \( |A| = C \) iff \( |A| = |R| \)

\( E1 \) The set of positive real numbers \( R^+ \) has cardinality \( C \) as function \( f \) given by a formula \( f(x) = 2^x \) for all \( x \in R \) is a 1-1 function and maps \( R \) onto \( R^+ \)

Theorem 2 The set \( 2^N \) is uncountable
Proof in the book p.28

Theorem 3 The set \( 2^N \) of all subsets of natural numbers has cardinality \( C \), i.e. \( |2^N| = C \)

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

**Definition**  $|A| \leq |B|$  iff  $A \sim C$ and $C \subseteq B$

Directly from the definition we have that

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

**Definition**  $|A| < |B|$  iff  $|A| \leq |B|$ and $|A| \neq |B|$

We have that $|N| = \aleph_0$, $C = |R|$, and $N \subseteq R$ hence from Fact 6, $\aleph_0 \leq C$, but $\aleph_0 \neq C$, hence we have

**Fact 7**  $\aleph_0 < C$
Uncountable Sets of Cardinality Greater than $C$

By **Cantor Theorem** we have that

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

and all sets

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

are uncountable with cardinality greater than $C$, as only

$$|\mathcal{P}(N)| = |R| = C$$
Countable and Uncountable Sets
Some Theorem and Facts

**Union 1**  Union of two infinitely countable sets is an infinitely countable set
\[ \mathbb{N}_0 + \mathbb{N}_0 = \mathbb{N}_0 \]

**Union 2**  Union of a finite (cardinality \( n \)) and infinitely countable set is an infinitely countable set
\[ \mathbb{N}_0 + n = \mathbb{N}_0 \]

**Union 3**  Union of an infinitely countable set and a set of the same cardinality as real numbers has the same cardinality as the set of real numbers
\[ \mathbb{N}_0 + C = C \]

**Union 4**  Union of two sets of cardinality the same as real numbers has the same cardinality as the set of real numbers
\[ C + C = C \]
Countable and Uncountable Sets
Some Theorem and Facts

**Cartesian Product 1** Cartesian Product of two infinitely countable sets is an infinitely countable set
\[ \mathbb{N}_0 \cdot \mathbb{N}_0 = \mathbb{N}_0 \]

**Cartesian Product 2** Cartesian Product of a non-empty finite set and an infinitely countable set is an infinitely countable set
\[ n \cdot \mathbb{N}_0 = \mathbb{N}_0 \quad \text{for} \quad n > 0 \]

**Cartesian Product 3** Cartesian Product of an infinitely countable set and a set of the same cardinality as real numbers has the same cardinality as the set of real numbers
\[ \mathbb{N}_0 \cdot C = C \]

**Cartesian Product 4** Cartesian Product of two sets of cardinality the same as real numbers has the same cardinality as the set of real numbers
\[ C \cdot C = C \]
Countable and Uncountable Sets
Some Theorem and Facts

**Power 1**  The set of all subsets of natural numbers (or any countably infinite set) has the same cardinality as the set of real numbers
\[ 2^{\aleph_0} = C \]

**Power 2**  There are \( C \) of all functions that map \( N \) into \( N \)

**Power 3**  There are \( C \) possible sequences that can be form out of an infinitely countable set
\[ \aleph_0^{\aleph_0} = C \]

**Power 4**  There are \( C^C \) of all functions that map \( R \) into \( R \)

**Power 5**  The set of all real functions of one variable has the same cardinality as the set of all subsets of real numbers
\[ C^C = 2^C \]
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 $A \subseteq R$ ($R$ 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 $2^N$ 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
Q1  Set $A$ is uncountable iff $A \subseteq \mathbb{R}$ (\(\mathbb{R}\) is the set of real numbers)

**NO**

The set $2^\mathbb{R}$ is uncountable, as $|\mathbb{R}| < |2^\mathbb{R}|$ by **Cantor Theorem** but $2^\mathbb{R}$ is not a subset of $\mathbb{R}$

Also $\mathbb{N} \subseteq \mathbb{R}$ and $\mathbb{N}$ is not uncountable
Answers to Simple Short Questions

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

NO

For example $A = \{\emptyset\}$ is countable as it is finite, but $\mathbb{N} \not\subseteq \{\emptyset\}$.

In fact $A$ can be any finite set, or any infinite set that does not include $\mathbb{N}$, for example $A = \{\{n\} : n \in \mathbb{N}\}$. 
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

$\{n \in N : n^2 + 1 \leq 15\} = \{0, 1, 2, 3\}$, hence

$A = \{\{0\}, \{1\}, \{2\}, \{3\}\}$ is a finite set
Q5 The set $A = \{(\{n\}, n) \in 2^N \times N : 1 \leq n \leq n^2\}$ is infinitely countable (countably infinite)

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 infinitely countable

The set $C = \{\{n\} \in 2^N : 1 \leq n \leq n^2\}$ is also 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 infinitely countable as a cartesian product of two infinitely countable sets (stated before and to be proved in the next section)
Countably Infinite Sets: Two Proofs

We have proved

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

We use it now to prove some Theorems about 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 as follows

$$A = \{a_0, a_1, a_2, \ldots\} \quad B = \{b_0, b_1, b_2, \ldots\}$$

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
Countably Infinite Sets: Two Proofs

**Cartesian Product Theorem**

*Cartesian Product 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 as follows:

$A = \{a_0, a_1, a_2, \ldots\}$ \quad $B = \{b_0, b_1, b_2, \ldots\}$ \quad We list their Cartesian Product $A \times B$ an infinite table as follows:

$(a_0, b_0), (a_0, b_1), (a_0, b_2), (a_0, b_3), \ldots$

$(a_1, b_0), (a_1, b_1), (a_1, b_2), (a_1, b_3), \ldots$

$(a_2, b_0), (a_2, b_1), (a_2, b_2), (a_2, b_3), \ldots$

$(a_3, b_0), (a_3, b_1), (a_3, b_2), (a_3, b_3), \ldots$

$\ldots, \ldots, \ldots, \ldots, \ldots,$
Cartesian Product Theorem Proof

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

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

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

$A \times B$ becomes now the following 1-1 sequence

$$(a_0, b_0), (a_1, b_0), (a_0, b_1), (a_2, b_0), (a_1, b_1), (a_0, b_2),$$

$$(a_3, b_0), (a_2, b_1), (a_1, b_2), (a_0, b_3),$$

$$\ldots, (a_3, b_1), (a_2, b_2), (a_1, b_3), \ldots, \ldots, \ldots, \ldots,$$

We prove by Mathematical induction that the sequence is well defined for all $n \in \mathbb{N}$ and hence that $|A \times B| = |\mathbb{N}|$

It ends the proof of the **Cartesian Product Theorem**

**Observe** that our both theorems can be generalized by Mathematical Induction to the case of sums or Cartesian Products of any finite number of sets
CHAPTER 1
PART 5: Fundamental Proof Techniques

1. Mathematical Induction
2. The Pigeonhole Principle
3. The Diagonalization Principle
Counting Functions Theorem
For any finite, non empty sets $A, B$, there are $|B|^{|A|}$ functions that map $A$ into $B$

Proof by Mathematical Induction over the number of elements of the set $A$, i.e. over $n \in \mathbb{N} - \{0\}$, where $n = |A|$

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

$$A = \{ a \}, \ B = \{ b_1, ... b_m \}, \ m \geq 1$$

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

$$f_1(a) = b_1, \ f_2(a) = b_2, \ ...., \ f_m(a) = b_m$$
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

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

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
Pigeonhole Principle Theorem Proof

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

\[
g : A - \{a\} \rightarrow B - \{f(a)\}
\]

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

\[
g(x) = f(x) \quad \text{for all } x \in A
\]

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

$$2^N$$ 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