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

if and only if there is a **bijection** function $f: A \longrightarrow B$,

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

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

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:

$$|A| = |B| \quad \text{or} \quad cardA = cardB$$

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

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

Finite and Infinite Sets

Definition

A set A is **finite** if and only if

there is $n \in N$ and there is a function

$$f: \{0, 1, 2, ..., n-1\} \stackrel{1-1, onto}{\longrightarrow} A$$

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 N of natural numbers is infinite

Consider a function f given by a formula

$f(n) = 2n$ for all $n \in N$

Obviously

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

By **Dedekind Theorem** the set N is infinite as the set 2N of even numbers are a proper subset of natural numbers N

Infinite Sets Examples

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

$$|N| = \aleph_0$$

Countably Infinite Sets

Definition

For any set A,

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

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

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

$$A: \ a_0,\ a_1,\ a_2, \dots \quad \text{and} \quad B: \ b_0,\ b_1,\ b_2, \dots$$

and their **union** can be listed as 1-1 sequence

$$A \cup B: \ a_0,\ b_0,\ a_1,\ b_1,\ a_2, b_2, \dots, \dots$$

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

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

$$\begin{array}{l} (a_0, b_0),\ (a_0, b_1),\ (a_0, b_2),\ (a_0, b_3),\ \ldots \\ (a_1, b_0),\ (a_1, b_1),\ (a_1, b_2),\ (a_1, b_3),\ \ldots \\ (a_2, b_0),\ (a_2, b_1),\ (a_2, b_2),\ (a_2, b_3),\ \ldots \\ (a_3, b_0),\ (a_3, b_1),\ (a_3, b_2),\ (a_3, b_3),\ \ldots \\ \ldots,\quad \ldots,\quad \ldots,\quad \ldots,\quad \ldots,\quad \ldots, \end{array}$$

Cartesian Product Theorem Proof

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

$$(a_0, b_0),\ (a_0, b_1),\ (a_0, b_2),\ (a_0, b_3),\ (a_0, b_4),\ \ldots, \ldots$$
$$(a_1, b_0),\ (a_1, b_1),\ (a_1, b_2),\ (a_1, b_3),\ \ldots$$
$$(a_2, b_0),\ (a_2, b_1),\ (a_2, b_2),\ (a_2, b_3),\ \ldots$$
$$(a_3, b_0),\ (a_3, b_1),\ (a_3, b_2),\ (a_3, b_3),\ \ldots$$
$$\ldots, \quad \ldots, \quad \ldots, \quad \ldots,$$

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), $\ldots$,

$\ldots, \quad \ldots, \quad \ldots, \quad \ldots,$

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 $\mathcal{C}$ - Continuum

We denote by $\mathcal{C}$ the cardinality of the set R of real numbers

$\mathcal{C}$ is a new **cardinal number** called continuum and we write

$$|R| = \mathcal{C}$$

Definition

We say that a set A has **cardinality** $\mathcal{C}$ (continuum)

if and only if $|A| = |R|$

We write it

$$|A| = \mathcal{C}$$

Sets of Cardinality $\mathcal{C}$

Example

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

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

is 1-1 function and maps R **onto** the set R^+

Sets of Cardinality $\mathcal{C}$

Theorem 2

The set 2^N of all subsets of natural numbers is **uncountable**

Proof

We prove it in PART 5 (book page 28)

Theorem 3

The set 2^N has cardinality $\mathcal{C}$, i.e.

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

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

Hence we proved

Fact 7

$$\aleph_0 < \mathcal{C}$$

Uncountable Sets of Cardinality Greater then $\mathcal{C}$

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

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

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

$$\aleph_0 < \mathcal{C} < |\mathcal{P}(\mathcal{P}(\mathcal{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{N})))| < \ldots$$

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

$$\aleph_0 + n = \aleph_0$$

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 $\mathcal{C}$ has the same cardinality as the set of real numbers

This means that

$$\aleph_0 + \mathcal{C} = \mathcal{C}$$

Union 4 Union of two sets of cardinality the same as real numbers (of cardinality $\mathcal{C}$) has the same cardinality as the set of real numbers

This means that

$$\mathcal{C} + \mathcal{C} = \mathcal{C}$$

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

$$n \cdot \aleph_0 = \aleph_0 \quad \text{for} \quad n > 0$$

Product 3

Cartesian Product of an infinitely countable set and an uncountable set of cardinality $\mathcal{C}$ has the cardinality $\mathcal{C}$

$$\aleph_0 \cdot \mathcal{C} = \mathcal{C}$$

Product 4

Cartesian Product of two uncountable sets of cardinality $\mathcal{C}$ has the cardinality $\mathcal{C}$

$$\mathcal{C} \cdot \mathcal{C} = \mathcal{C}$$

Countable and Uncountable Sets

Power 1

The set 2^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 C of all functions that map N into 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 R into 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

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

Theorem 4

$$n < \aleph_0 < \mathcal{C}$$

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

$$\text{If} \quad |A| = n,\ n \geq 1, \quad \text{then} \quad |A^*| = \aleph_0$$

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

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

Answers to Simple Short Questions

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

$$N \not\subseteq \{\emptyset\}$$

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

$|2^N| = |R| = \mathcal{C}$ 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**

Answers to Simple Short Questions

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 **nfinitely 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 the Cartesian Product of two infinitely countable sets

CHAPTER 1

PART 5: Fundamental Proof Techniques

1. Counting Functions Theprem
2. The Pigeonhole Principle
3. The Diagonalization Principle

Mathematical Induction Applications 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.

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

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 $f : \{a\} \longrightarrow \{b_1, ...b_m\}$ defined as follows

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

Counting Functions Theorem Proof

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

$$f : A \longrightarrow B = \{b_1, ...b_m\}$$

We **group** all functions that map A_1 as follows

Group 1 contains all functions f_1 such that

$$f_1 : A \longrightarrow B$$

and they have the following property

$$f_1(a) = b_1, \ \ f_1(x) = f(x) \quad \text{for all} \quad f : A \longrightarrow B \ \text{and} \ x \in A_1$$

By inductive assumption there are m^n functions in the **Group** 1

Inductive Step

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

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

$$f_i : A \longrightarrow B$$

and they have the following property

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

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

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**

Pigeonhole Principle Theorem

If A and B are non-empty finite sets and $|A| > |B|$,

then **there is no** one-to one function from A to B

Proof

We conduct the proof by by Mathematical Induction over

$n \in N - \{0\}$, where $n = |B|$ and $B \neq \emptyset$

Base case $n = 1$

Suppose $|B| = 1$, that is, $B = \{b\}$, and $|A| > 1$.

If $f : A \longrightarrow \{b\}$,

then there are at least two distinct elements $a_1, a_2 \in A$, such that $f(a_1) = f(a_2) = \{b\}$

Hence the function f **is not** one-to one

Pigeonhole Principle Proof

Inductive Assumption

We assume that any $f : A \longrightarrow B$ is **not one-to one** provided

$$|A| > |B| \quad \text{and} \quad |B| \leq n, \quad \text{where} \quad n \geq 1$$

Inductive Step

Suppose that $f : A \longrightarrow B$ is such that

$$|A| > |B| \quad \text{and} \quad |B| = n + 1$$

Choose some $b \in B$

Since $|B| \geq 2$ we have that $B - \{b\} \neq \emptyset$

Pigeonhole Principle Proof

Consider the set $f^{-1}(\{b\}) \subseteq A$. We have two cases

1. $|f^{-1}(\{b\})| \geq 2$

Then by definition there are $a_1, a_2 \in A$,

such that $a_1 \neq a_2$ and $f(a_1) = f(a_2) = b$ what proves that the function f **is not** one-to one

2. $|f^{-1}(\{b\})| \leq 1$

Then we consider a function

$$g : \; A - f^{-1}(\{b\}) \longrightarrow B - \{b\}$$

such that

$$g(x) = f(x) \quad \text{for all} \quad x \in A - f^{-1}(\{b\})$$

Pigeonhole Principle Proof

Observe that the inductive assumption **applies** to the function g because $|B - \{b\}| = n$ for $|B| = n + 1$ and

$$|A - f^{-1}(\{b\})| \geq |A| - 1 \text{ for } |f^{-1}(\{b\})| \leq 1$$

We know that $|A| > |B|$, so

$|A| - 1 > |B| - 1 = n = |B - \{b\}|$ and $|A - f^{-1}(\{b\})| > |B - \{b\}|$

By the inductive assumption applied to g we get that

g **is not** one -to one

Hence $g(a_1) = g(a_2)$ for some distinct
$a_1, a_2 \in A - f^{-1}(\{b\})$,

but then $f(a_1) = f(a_2)$ and f **is not** one -to one either

Pigeonhole Principle Revisited

We now formulate a bit stronger version of the the pigeonhole principle and present its slightly different proof

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

We conduct the proof by by Mathematical Induction over $n \in N$, where $n = |B|$

Base case $n = 0$

Assume $|B| = 0$, that is, $B = \emptyset$. Then **there is no** function $f : A \longrightarrow B$ whatsoever; let alone a one-to one function

Pigeonhole Principle Revisited Proof

Inductive Assumption

Any function $f : A \longrightarrow B$ is **not one-to one** provided

$$|A| > |B| \quad \text{and} \quad |B| \leq n, \quad n \geq 0$$

Inductive Step

Suppose that $f : A \longrightarrow B$ is such that

$$|A| > |B| \quad \text{and} \quad |B| = n + 1$$

We have to show that f is **not one-to one** under the Inductive Assumption

Pigeonhole Principle Revisited Proof

We proceed as follows

We **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 $a' \neq a$ and $f(a) = f(a')$, then obviously the function f is **not one-to one** and we are done

So, **suppose now** that the chosen $a \in A$ is **the only** element mapped by f to f(a)

Pigeonhole Principle Revisited Proof

Consider then the sets $A - \{a\}$ and $B - \{f(a)\}$ and a function

$$g : \; A - \{a\} \longrightarrow B - \{f(a)\}$$

such that

$$g(x) = f(x) \quad \text{for all} \quad x \in A - \{a\}$$

Observe that the Inductive Assumption applies to g because

$$|B - \{f(a)\}| = n \quad \text{and}$$

$$|A - \{a\}| = |A| - 1 > |B| - 1 = |B - \{f(a)\}|$$

Pigeonhole Principle Revisited Proof

Hence by the inductive assumption the function

g is **not one-to one**

Therefore, there are two distinct elements elements of

$A - \{a\}$ that are mapped by g to the same element of

$B - \{f(a)\}$

The function g is, by definition, such that

$$g(x) = f(x) \quad \text{for all} \quad x \in A - \{a\}$$

so the function f is **not one-to one** either

This **ends** the proof

Pigeonhole Principle Application

The Pigeonhole Principle is used in a large variety of proofs including many in this course

Here is one simple application to be used in later Chapters

Path 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 $i = 1, \ldots, n-1$ 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** 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 Principle which justifies a new important proof technique

Diagonalization Principle (Georg Cantor 1845-1918)

Let R be a binary relation on a set A , i.e.

$R \subseteq A \times A$ 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

Here are two theorems whose proofs are the ”classic” applications of the Diagonalization Principle

Cantor Theorem 2

Let N be the set on natural numbers

The set 2^N **is uncountable**

Cantor Theorem 3

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

Cantor Theorem 2
Let N be the set on natural numbers

The set 2^N **is uncountable**

Proof
We apply proof by contradiction method and the Diagonalization Principle
Suppose that 2^N is **countably infinite**. That is, we assume that we can put sets of 2^N in a one-to one sequence $\{R_n\}_{n \in N}$ such that

$$2^N = \{R_0,\ R_1,\ R_2,\ \dots\}$$

We define a binary relation $R \subseteq N \times N$ as follows

$$R = \{(i, j) :\ j \in R_i\}$$

This means that for any $i, j \in N$ we have that

$$(i, j) \in R \text{ if and only if } j \in R_i$$

Cantor Theorem 2 Proof

In particular, for any $i, j \in N$ we have that

$$(i, j) \notin R \quad \text{if and only if} \quad j \notin R_i$$

and the **diagonal set** D for R is

$$D = \{n \in N : \quad n \notin R_n\}$$

By definition $D \subseteq N$, i.e.

$$D \in 2^N = \{R_0,\ R_1,\ R_2,\ \dots\}$$

and hence

$$D = R_k \quad \text{for some} \quad k \geq 0$$

Cantor Theorem 2 Proof

We obtain **contradiction** by asking whether $k \in R_k$ for

$$D = R_k$$

We have two cases to consider: $k \in R_k$ or $k \notin R_k$

c1 Suppose that $k \in R_k$

Since $D = \{n \in N : \ n \notin R_n\}$ we have that $k \notin D$

But $D = R_k$ and we get $k \notin R_k$

Contradiction

c2 Suppose that $k \notin R_k$

Since $D = \{n \in N : \ n \notin R_n\}$ we have that $k \in D$

But $D = R_k$ and we get $k \in R_k$

Contradiction

This ends the **proof**

Cantor Theorem 3

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

Proof

We carry the proof by the contradiction method

We assume hat the set of real numbers in the interval $[0, 1]$ is **infinitely countable**

This means, by definition , that there is a function f such that

$f : N \xrightarrow{1-1, onto} [01]$

Let f be any such function. We write $f(n) = d_n$ and denote by

$$d_0, \; d_1, \; \ldots, \; d_n, \; \ldots,$$

a sequence of of **all elements** of $[01]$ **defined** by f

We will get a **contradiction** by showing that one can always find an element $d \in [01]$ such that $d \neq d_n$ for all $n \in N$

Cantor Theorem 3 Proof

We use **binary** representation of real numbers

Hence we assume that all numbers in the interval [01] form a one to one sequence

$$d_0 = 0.a_{00}\ a_{01}\ a_{02}\ a_{03}\ a_{04}\ \ \dots\ \ \dots$$

$$d_1 = 0.a_{10}\ a_{11}\ a_{12}\ a_{13}\ a_{04}\ \ \dots\ \ \dots$$

$$d_2 = 0.a_{20}\ a_{21}\ a_{22}\ a_{23} a_0\ \ \dots\ \ \dots$$

$$d_3 = 0.a_{30}\ a_{31}\ a_{32}\ a_{33}\ a_{04} \dots\ \ \dots$$

$$\dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots$$

where all $a_{ij} \in \{0, 1\}$

Cantor Theorem 3 Proof

We use Cantor Diagonatization idea to define an element $d \in [01]$, such that $d \neq d_n$ for all $n \in N$ as follows

For each element a_{nn} of the "diagonal"

$$a_{00}, \ a_{11}, \ a_{22}, \ \ldots \ \ a_{nn}, \ \ldots \ \ , \ \ldots$$

of the sequence $d_0, \ d_1, \ \ldots, \ \ d_n, \ \ldots,$ of binary representation of all elements of the interval $[01]$ we define an element $b_{nn} \neq a_{nn}$ as

$$b_{nn} = \begin{cases} 0 & \text{if } a_{nn} = 1 \\ 1 & \text{if } a_{nn} = 0 \end{cases}$$

Cantor Theorem 3 Proof

Given such defined sequence

$$b_{00},\ b_{11},\ b_{22},\ b_{33},\ b_{44},\ \ldots\ \ldots$$

We now construct a real number d as

$$d = b_{00}\ b_{11}\ b_{22}\ b_{33}\ b_{44}\ \ \ldots\ \ldots$$

Obviously $d \in [01]$ and by the Diagonatization Principle

$d \neq d_n$ for all $n \in N$

Contradiction

This ends the **proof**

Cantor Theorem 3 Proof

Here is **another proof** of the Cantor Theorem 3

It uses, after Cantor the **decimal representation** of real numbers

In this case we assume that all numbers in the interval [01] form a one to one sequence

$$d_0 = 0.a_{00}\ a_{01}\ a_{02}\ a_{03}\ a_{04}\ \ \dots\ \ \dots$$

$$d_1 = 0.a_{10}\ a_{11}\ a_{12}\ a_{13}\ a_{04}\ \ \dots\ \ \dots$$

$$d_2 = 0.a_{20}\ a_{21}\ a_{22}\ a_{23} a_0\ \ \dots\ \ \dots$$

$$d_3 = 0.a_{30}\ a_{31}\ a_{32}\ a_{33}\ a_{04} \dots\ \ \dots$$

$$\dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots\ \ \dots$$

where all $a_{ij} \in \{0, 1, 2 \dots 9\}$

Cantor Theorem 3 Proof

For each element a_{nn} of the "diagonal"

$$a_{00},\ a_{11},\ a_{22},\ \ldots\ a_{nn},\ \ldots\ ,\ \ldots$$

we define now an element (this is not the only possible definition) $b_{nn} \neq a_{nn}$ as

$$b_{nn} = \begin{cases} 2 & \text{if } a_{nn} = 1 \\ 1 & \text{if } a_{nn} \neq 1 \end{cases}$$

We construct a real number $d \in [01]$ as

$$d = b_{00}\ b_{11}\ b_{22}\ b_{33}\ b_{44}\ \ \ldots\ \ \ldots$$