cse581
COMPUTER SCIENCE FOUNDAMENTALS: THEORY

Professor Anita Wasilewska

Lecture 4

DISCRETE MATHEMATICS BASICS

Discrete Mathematics Basics

PART 5: Some Fundamental Proof Techniques

Theory of Computation BASICS

PART 6: Closures and Algorithms

PART 7: Alphabets and languages

PART 8: Finite Representation of Languages

Discrete Mathematics Basics

PART 5: Fundamental Proof Techniques

1. Mathematical Induction
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

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

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

Counting Functions Theorem Proof

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

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

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**

Mathematical Induction Applications
Pigeonhole Principle

Pigeonhole Principle Theorem

If A and B are non-empy 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

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

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 Theorem Application

The **Pigeonhole Principle Theorem** is a quite simple fact but is used in a large variety of proofs. We present here just one simple application which we will use in later **B2** 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 $i = 1, 2, \ldots n - 1$ 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 $(a_n, a_1) \in R$

Pigeonhole Principle Theorem Application

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

$$R_a = \{b \in A : \quad (a, b) \in R\}$$

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 Proof

Cantor Theorem 2

Let N be the set on natural numbers

$$\text{The set } 2^N \textbf{ is uncountable}$$

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

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

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.

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

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

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

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

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

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

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

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

$$\ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots$$

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

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

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

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

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

$$\ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots$$

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

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

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