Cse303
INTRODUCTION TO THE THEORY OF COMPUTATION
LECTURE NOTES

Professor Anita Wasilewska
Stony Brook University (SUNY at Stony Brook)

Course Text Book

ELEMENTS OF THE THEORY OF COMPUTATION

Harry R. Lewis, and Christos H. Papadimitriou

Prentice Hall, 2nd Edition

LECTURE 1

Course Web Page
www3.cs.stonybrook.edu/~ cse303

The course webpage contains the course **Lectures Slides** and a set of **Chapters Video Slides**

The **Lectures** follow the course **Textbook** very closely and supplement it by providing detailed definition and explanations of the material, additional problems with solutions, new examples, and detailed **solutions** to majority of the Textbook homework problems;

It also has a lot of previous quizzes and tests **solution** to be used by students to study and learn from

Course Objectives

The main objective of the course is to introduce abstract models of computation such as finite and push-down automata, and analyze their **relationship** and relative expressive power

We will explore the connection between abstract machine models and formal languages, as specified by grammars

The **course** will enhance students' awareness of both the power and inherent imitations of **algorithmic computation** via the study of Turing machines and/or other abstract **computational models**

CHAPTER 1
Discrete Mathematics Basics

PART 0: Basic sets of Numbers, Peano Arithmetic

PART 1: Sets and Operations on Sets

PART 2: Relations and Functions

PART 3: Special types of Binary Relations

PART 4: Finite and Infinite Sets

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

CHAPTER 1

Discrete Mathematics Basics

PART 0: Basic sets of Numbers, Peano Arithmetic

Basic Sets of Numbers

Natural numbers N, Integers Z, Positive Integers Z^+, Positive Natural numbers N^+, Prime Numbers P, Rational Numbers Q, and Real numbers R

Natural Numbers N

$$N = \{0,\ 1,\ 2,\ 3,\ \ldots,\ \ldots\}$$

Integers Z and Positive Integers Z^+

$$Z = \{\ \ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots,\ \ldots\}$$

$$Z^+ = \{\ 1,\ 2,\ 3,\ \ldots,\ \ldots\}$$

Positive Integers Z^+ are also called Positive Natural numbers N^+ and we denote

$$N^+ = \{\ 1,\ 2,\ 3,\ \ldots,\ \ldots\}$$

Prime Numbers

A positive integer $p \in Z^{+}$ is called prime
if it has only two divisors, namely 1 and p
By convention, 1 **is not** prime

Prime Numbers P

$$P = \{ 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ \ldots, \ \ldots \}$$

Rational and Real Numbers

Rational numbers Q

$$Q = \{\frac{p}{q} : \quad p, q \in Z \quad \text{and} \quad q \neq 0\ \}$$

Real numbers R

The **first rigorous definition** of the set R of real numbers was published by **Cantor** in 1871

Cantor's definition (as established today in modern terminology)

The set R Is the **quotient set** of the set of Cauchy sequences of **rational numbers**, with two sequences considered **equivalent** if their difference converges to zero

Cantor also showed In 1874, that the set of all **real numbers** is uncountably infinite, but the set of all **algebraic numbers** is countably infinite

Real Numbers

The **other first rigorous definition** of R established today was given by **Richard Dedekind** at the same time and independent from **Cantor** in terms what we call now Dedekind cuts

The concept of theDedekind cuts developed for it became on of the very important concepts for modern mathematics

The set of R is often called ”The Reals” - after the name ”real numbers” **first used** by a French philosopher, scientist, and mathematician **Rene Descartes** (1596 -1650), also known as **Renatus Cartesius**

Irrational and Algebraic Numbers

Of course we have that $N \subset Q \subset R$

Real numbers that are not Rational are called **Irrational** numbers, i.e. we put $IR = R - Q$

Algebraic number is a number that is a **root** of a non-zero polynomial P(x) in one variable equation P(x) = 0 with **integer** (or, equivalently **rational**) coefficients

All **rational** numbers are **algebraic**

Let $x \in Q$, by the definition $x = \frac{a}{b}$ for any integers $a, b \neq 0$ is the root of a non-zero polynomial equation namely $bx - a = 0$

Encyclopedia Britannica

Here is what is published the Encyclopedia Britannica

Real number in mathematics, is a quantity that can be expressed as an infinite decimal expansion

The real numbers include the positive and negative integers and the fractions made from those integers (or rational numbers) and**also** the irrational numbers

Natural Numbers in Encyclopedia Britannica

Here is what is published the Encyclopedia Britannica

Natural numbers: called the counting numbers or natural numbers $1, 2, 3, \ldots\ldots$ For an empty set, no object is present, and the **count yields** the number 0, which, appended to the counting numbers, produces what are known as the **whole numbers**

Hence the Modern Mathematics definition is

$$N = \{0, 2, 3, 4, \ldots \; \ldots\}$$

$$N = Z^{+} \cup \{0\} = N^{+} \cup \{0\} = \textbf{ whole numbers}$$

Peano Arithmetic PA

Next to geometry, the **theory of natural numbers** is the most intuitive and intuitively known of all branches of mathematics

This is why the first attempts to **formalize mathematics** begin with arithmetic of natural numbers.

The first attempt of axiomatic formalization was given by Dedekind in **1879** and by Peano in **1889**

The Peano formalization became known as **Peano Postulates** and can be written as follows.

Peano Arithmetic PA

Peano Postulates (1889)

p1 0 is a natural number

p2 If n is a natural number, there is another number which we denote by n'
We call the number n' a **successor** of n and the intuitive meaning of n' is $n + 1$

p3 $0 \neq n'$, for any natural number n

p4 If $n' = m'$, then $n = m$, for any natural numbers n, m

Peano Arithmetic PA

p5 **If** W is is a property that may or may not hold for natural numbers, and
if **(i)** 0 has the property W and
(ii) whenever a natural number n has the property W, then n' has the property W,
then all natural numbers have the property W

The postulate **p5** is called Principle of Induction

Peano Arithmetic PA

The **Peano Postulates** together with certain amount of set theory are sufficient to develop **not only** theory of natural numbers, **but also** theory of rational and even real numbers

But **Peano Postulates** can't act as a fully formal theory as they include **intuitive** notions like "property" and "has a property"

A **formal theory** of natural numbers based on the Peano Postulates is referred in literature as **Peano Arithmetic**, or simply PA

The full rigorous formalization by Mendelson (1973) is included and worked out in the smallest **details** in his book *Intoduction to Mathematical Logic* (1987)

Chapter 1

PART 1: Sets and Operations on Sets

Sets

Set A set is a collection of objects

Elements The objects comprising a set are are called its elements or members

$a \in A$ denotes that a is an **element** of a set A

$a \notin A$ denotes that a is not an **element** of A

Empty Set is a set without elements

Empty Set is denoted by $\emptyset$

Sets

Sets can be defined by listing their elements;

Example

The set

$$A = \{a, \emptyset, \{a, \emptyset\}\}$$

has 3 elements:

$$a \in A, \quad \emptyset \in A, \quad \{a, \emptyset\} \in A$$

Sets

Sets can be defined by referring to other sets and to **properties** P(x) that elements may or may not have

We write it as

$$B = \{x \in A : \quad P(x)\}$$

Example

Let N be a set of natural numbers

$$B = \{n \in N : \quad n < 0\} = \emptyset$$

Operations on Sets

Set Inclusion

$A \subseteq B$ if and only if $\forall a(a \in A \Rightarrow a \in B)$

is a **true** statement

Set Equality

$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$

Proper Subset

$A \subset B$ if and only if $A \subseteq B$ and $A \neq B$

Operations on Sets

Subset Notations

$A \subseteq B$ for a subset (might be improper)

$A \subset B$ for a proper subset

Power Set Set of all subsets of a given set

$$\mathcal{P}(A) = \{B : \quad B \subseteq A\}$$

Other Notation

$$2^A = \{B : \quad B \subseteq A\}$$

Operations on Sets

Union

$A \cup B = \{x : \quad x \in A \quad \text{or} \quad x \in B\}$

We write:

$x \in A \cup B$ if and only if $x \in A \ \cup \ x \in B$

Intersection

$A \cap B = \{x : \quad x \in A \quad \text{and} \quad x \in B\}$

We write:

$x \in A \cap B$ if and only if $x \in A \cap \ x \in B$

Operations on Sets

Relative Complement

$x \in (A - B)$ if and only if $x \in A$ and $x \notin B$

We write:

$$A - B = \{x : \; x \in A \cap x \notin B\}$$

Complement is defined only for $A \subseteq U$, where U is called an **universe**

$$-A = U - A$$

We write for $x \in U$,

$x \in -A$ if and only if $x \notin A$

Operations on Sets

Algebra of sets consists of properties of sets that are **true** for all sets involved

We use **tautologies** of propositional logic

to prove **basic** properties of the algebra of sets

We then use the basic properties to **prove** more elaborated properties of sets

Operations on Sets

It is possible to form intersections and unions of **more** then two, or even a finite number o **sets**

Let $\mathcal{F}$ denote is any **collection** of sets

We write $\bigcup \mathcal{F}$ for the **set** whose **elements** are the elements of **all** of the sets in $\mathcal{F}$

Example Let

$$\mathcal{F} = \{\{a\}, \{\emptyset\}, \{a, \emptyset, b\}\}$$

We get

$$\bigcup \mathcal{F} = \{a,\ \emptyset,\ b\}$$

Operations on Sets

Observe that given

$$\mathcal{F} = \{\{a\}, \{\emptyset\}, \{a, \emptyset, b\}\} = \{A_1,\ A_2,\ A_3\}$$

we have that

$$\{a\} \cup \{\emptyset\} \cup \{a, \emptyset, b\} = A_1 \cup\ A_2 \cup A_3 = \{a,\ \emptyset,\ b\} = \bigcup \mathcal{F}$$

Hence we have that for any element x,

$x \in \bigcup \mathcal{F}$ if and only if there exists i, such that $x \in A_i$

Operations on Sets

We **define** formally

Generalized Union of any family $\mathcal{F}$ of sets is

$$\bigcup \mathcal{F} = \{x : \text{ exists a set } S \in \mathcal{F} \text{ such that } x \in S\}$$

We write it also as

$$x \in \bigcup \mathcal{F} \quad \text{if and only if} \quad \exists_{S \in \mathcal{F}} \; x \in S$$

Operations on Sets

Generalized Intersection of any family $\mathcal{F}$ of sets is

$$\bigcap \mathcal{F} = \{x : \quad \forall_{S \in \mathcal{F}}\ x \in S\}$$

We write

$$x \in \bigcap \mathcal{F} \quad \text{if and only if} \quad \forall_{S \in \mathcal{F}}\ x \in S$$

Operations on Sets

Ordered Pair

Given two sets A, B we denote by

$$(a, b)$$

an **ordered pair**, where $a \in A$ and $b \in B$

We call a a **first** coordinate of (a, b)

and b its **second** coordinate

We define

$$(a, b) = (c, d) \quad \text{if and only if} \quad a = c \quad \text{and} \quad b = d$$

Operations on Sets

Cartesian Product

Given two sets A and B, the set

$$A \times B = \{(a, b) : \ a \in A \text{ and } b \in B\}$$

is called a **Cartesian (Cross)** Product) of the sets A, B

We write

$$(a, b) \in A \times B \quad \text{if and only if} \quad a \in A \text{ and } b \in B$$

In case when $A = B$, we have that

$$A \times A = \{(a, b) : \ a, b \in A\}$$

Chapter 1

PART 2 : Relations and Functions

Binary Relations

Binary Relation

Any set R such that $R \subseteq A \times B$

is called a **binary relation** defined in the **Cartesian (Cross)** Product of the sets A, B

Domain, Range of R

Given a binary relation $R \subseteq A \times B$, the set

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

is called a **domain** of the relation R

The set

$$V_R = \{b \in B : \quad (a, b) \in R\}$$

is called a **range** (set of values) of the relation R

Binary Relations

Binary Relation

Any set R such that $R \subseteq A \times A$

is called a **binary relation** defined in a set A

Domain, Range of R

Given a binary relation $R \subseteq A \times A$, the set

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

is called a **domain** of the relation R

The set

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

is called a **range** (set of values) of the relation R

n- ary Relations

Ordered tuple

Given sets $A_1, ...A_n$, an element $(a_1, a_2, ...a_n)$ such that $a_i \in A_i$ for $i = 1, 2, ...n$ is called an **ordered tuple**

Cartesian (Cross) Product of sets $A_1, , A_n$ is a set

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ...a_n) : \ a_i \in A_i, i = 1, 2, ...n\}$$

n-ary Relation

Any set R such that $R \subseteq A_1 \times A_2 \times \ \dots \ \times A_n$

is called **n-ary Relation** defined in the Cartesian (Cross) Product $A_1 \times A_2 \times ... \times A_n$

When $A_1 = A_2 = ... = A_n = A$ then $R \subseteq A \times A \ \dots \ \times A$

is called **n-ary Relation** defined in the set A

Function as Relation

Definition

A binary relation $R \subseteq A \times B$ is a **function** from A to B if and only if the following condition holds

$$\forall_{a \in A} \; \exists!_{\, b \in B} \; (a, b) \in R$$

where $\exists!_{\, b \in B}$ means there is **exactly one** $b \in B$

Because the condition says that for any $a \in A$ we have **exactly one** $b \in B$, we write

$$R(a) = b \quad \text{for} \quad (a,\ b) \in R$$

Function as Relation

Given a binary relation

$$R \subseteq A \times B$$

that is a **function**

The set A is called a **domain** of the function R
and we write:

$$R : \quad A \longrightarrow \quad B$$

to denote that the **relation** R is a **function** and say that
R **maps** the set A **into** the set B

Functions

Function notation

We denote relations that are functions by letters f, g, h,...
and write

$$f: \quad A \longrightarrow B$$

say that the function f **maps** the set A **into** the set B

Domain, Codomain

Let $f: \quad A \longrightarrow B,$

the set A is called a **domain** of f ,

and the set B is called a **codomain** of f

Range

Given a function $f: \quad A \longrightarrow B$

The set

$$R_f = \{b \in B : \quad b = f(a) \text{ and } a \in A\}$$

is called a **range** of the function f

By definition, the **range** of f is a subset of its **codomain** B

We write $R_f = \{b \in B : \quad \exists_{a \in A}\ b = f(a)\}$

The set

$$f = \{(a, b) \in A \times B : \quad b = f(a)\}$$

is called a **graph** of the function f

Functions

Function *"onto"*

The function $f: \ A \longrightarrow B$ is an **onto** function if and only if the following condition holds

$$\forall_{b \in B} \ \exists_{a \in A} \ f(a) = b$$

We denote it by

$$f: \ A \xrightarrow{onto} B$$

Functions

Function *" one- to -one"*

The function $f: \; A \longrightarrow B$

is called a **one- to -one** function and denoted by

$$f: \; A \xrightarrow{1-1} B$$

if and only if the following condition holds

$$\forall_{x,y \in A} (x \neq y \Rightarrow f(x) \neq f(y) \;)$$

Functions

A function $f: \ A \longrightarrow B$ is **not one- to -one** function if and only if the following condition holds

$$\exists_{x,y \in A}(x \neq y \cap f(x) = f(y)\ )$$

If a function f is **1-1** and **onto** we denote it as

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

Functions

Composition of functions

Let f and g be two functions such that

$$f: \quad A \longrightarrow B \quad \text{and} \quad g: \quad B \longrightarrow C$$

We **define** a new function

$$h: \quad A \longrightarrow C$$

called a **composition** of functions f and g as follows:

for any $x \in A$ we put

$$h(x) = g(f(x))$$

Composition notation

Given function f and g such that

$$f: \quad A \longrightarrow B \quad \text{and} \quad g: \quad B \longrightarrow C$$

We **denote** the **composition** of f and g by $(f \circ g)$
in order to stress that the function

$$f: \quad A \longrightarrow \mathbf{B}$$

"goes first" followed by the function

$$g: \quad \mathbf{B} \longrightarrow C$$

with a **shared** set **B** between them

Functions

We write now the **definition** of composition of functions f and g using the **composition notation** (name for the composition function) $(f \circ g)$ as follows

The composition $(f \circ g)$ is a **new** function

$$(f \circ g): \quad A \longrightarrow C$$

such that for any $x \in A$ we put

$$(f \circ g)(x) = g(f(x))$$

Functions

There is also other notation (name) for the **composition** of f and g that uses the symbol $(g \circ f)$, i.e. we put

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

This notation was invented to help calculus students to remember the formula g(f(x)) defining the composition of functions f and g

Functions

Inverse function

Let $f: \ A \longrightarrow B$ and $g: \ B \longrightarrow A$

g is called an **inverse** function to f if and only if the following condition holds

$$\forall_{a \in A} (f \circ g)(a) = g(f(a)) = a$$

If g is an **inverse** function to f we denote by $g = f^{-1}$

Functions

Identity function

A function $I: \quad A \longrightarrow A$ is called an **identity** on A if and only if the following condition holds

$$\forall_{a \in A} I(a) = a$$

Inverse and Identity

Let $f: \quad A \longrightarrow B$ and let $f^{-1}: \quad B \longrightarrow A$ be an **inverse** to f, then the following hold

$$(f \circ f^{-1})(a) = f^{-1}(f(a)) = I(a) = a, \quad \text{for all} \quad a \in A$$

$$(f^{-1} \circ f(b)) = f(f^{-1}(b) = I(b) = b, \quad \text{for all} \quad b \in B$$

Functions: Image and Inverse Image

Image

Given a function $f: \ X \longrightarrow Y$ and a set $A \subseteq X$

The set

$$f[A] = \{y \in Y : \quad \exists x \; (x \in A \;\cap\; y = f(x))\}$$

is called an **image** of the set $A \subseteq X$ **under** the function f

We write

$$y \in f[A] \quad \text{if and only if} \quad \text{there is} \quad x \in A \text{ and } y = f(x)$$

Other symbols used to denote the **image** are

$$f^{\rightarrow}(A) \quad \text{or} \quad f(A)$$

Functions: Image and Inverse Image

Inverse Image

Given a function $f: \; X \longrightarrow Y$ and a set $B \subseteq Y$

The set

$$f^{-1}[B] = \{x \in X : \; f(x) \in B\}$$

is called an **inverse image** of the set $B \subseteq Y$ **under** the function f

We write

$$x \in f^{-1}[B] \quad \text{if and only if} \quad f(x) \in B$$

Other symbol used to denote the **inverse image** are

$$f^{-1}(B) \quad \text{or} \quad f^{\leftarrow}(B)$$

Sequences

Definition

A **sequence** of elements of a set A is any **function** from the set of natural numbers N into the set A, i.e. any function

$$f: \; N \longrightarrow A$$

Any $f(n) = a_n$ is called **n-th term** of the sequence f

Notations

$$f = \{a_n\}_{n \in N}, \quad \{a_n\}_{n \in N}, \quad \{a_n\}$$

Sequences Example

Example

We define a **sequence f** of real numbers R as follows

$$f : \quad N \longrightarrow R$$

such that

$$f(n) = n + \sqrt{n}$$

We also use a shorthand notation for the function f and write it as

$$a_n = n + \sqrt{n}$$

Sequences Example

We often write the function $f = \{a_n\}$ in an even shorter and **informal** form as

$$a_0 = 0, \quad a_1 = 1 + 1 = 2, \quad a_2 = 2 + \sqrt{2}.........$$

or even as

$$0, \quad 2, \quad 2 + \sqrt{2}, \; 3 + \sqrt{3}, \; ....n + \sqrt{n}.........$$

Observations

Observation 1

By definition, **sequence** of elements of any set is always infinite (countably infinite) because the domain of the **sequence** function f is a set N of **natural numbers**

Observation 2

We can enumerate elements of a **sequence** by any **infinite** subset of N

We usually take a set $N - \{0\}$ as a **sequence** domain (enumeration)

Observations

Observation 3

We can choose as a set of indexes of a **sequence** any countably infinite set T, i. e, **not only** the set N of natural numbers

We often choose $T = N - \{0\} = N^+$, i.e we consider **sequences** that "start" with $n = 1$

In this case we write sequences as

$$a_1, \quad a_2, \quad a_3, \quad ..... \quad a_n, \ \ldots \ \ldots$$

Finite Sequences

Finite Sequence

Given a finite set $K = \{1, 2, \ \ldots, \ n\}$, for $n \in N$ and any set A

Any function

$$f : \{1, 2, ...n\} \longrightarrow A$$

is called a **finite sequence** of elements of the set A of the **length** n

Case n=0

In this case the function f is an empty set and we call it an **empty sequence**

We denote the empty sequence by e

Example

Consider a sequence given by a formula

$$a_n = \frac{n}{(n-2)(n-5)}$$

The domain of the function $f(n) = a_n$ is the set $N - \{2, 5\}$ and the **sequence** f is a function

$$f : \quad N - \{2, 5\} \;\rightarrow\; R$$

The **first** elements of the **sequence** f are

$$a_0 = f(0),\; a_1 = f(1),\; a_3 = f(3),\; a_4 = f(4)\; a_5 = f(5),\; a_6 = f(6), \dots$$

Example

Let $T = \{-1, -2, 3, 4\}$ be a **finite** set and

$$f : \{-1, -2, 3, 4\} \rightarrow R$$

be a function given by a formula

$$f(n) = a_n = \frac{n}{(n-2)(n-5)}$$

f is a finite sequence of **length** 4 with elements

$$a_{-1} = f(-1), \quad a_{-2} = f(-2), \quad a_3 = f(3), \quad a_4 = f(4)$$

Families of Sets Revisited

Family of sets

Any collection of sets is called a **family of sets**

We denote the family of sets by

$$\mathcal{F}$$

Sequence of sets

Any function

$$f : \ N \longrightarrow \mathcal{F}$$

is a **sequence of sets**, i..e a sequence where all its elements are sets

We use capital letters to denote sets and write the **sequence** of sets as

$$\{A_n\}_{n \in N}$$

Generalized Union

Generalized Union

Given a sequence $\{A_n\}_{n \in N}$ of sets

We define that **Generalized Union** of the sequence of sets as

$$\bigcup_{n \in N} A_n = \{x : \ \exists_{n \in N} \ x \in A_n\}$$

We write

$$x \in \bigcup_{n \in N} A_n \quad \text{if and only if} \quad \exists_{n \in N} \ x \in A_n$$

Generalized Intersection

Given a sequence $\{A_n\}_{n \in N}$ of sets

We define that **Generalized Intersection** of the sequence of sets as

$$\bigcap_{n \in N} A_n = \{x : \ \forall_{n \in N} \, x \in A_n\}$$

We write

$$x \in \bigcap_{n \in N} A_n \quad \text{if and only if} \quad \forall_{n \in N} \, x \in A_n$$

Indexed Family of Sets

Indexed Family of Sets

Given $\mathcal{F}$ be a family of sets

Let $T \neq \emptyset$ be any non empty set

Any function

$$f: \quad T \longrightarrow \mathcal{F}$$

is called an indexed family of sets with the set of indexes T

We write it

$$\{A_t\}_{t \in T}$$

Notice

Any sequence of sets is an indexed family of sets for T = N

Chapter 1

Some Simple Questions and Answers

Simple Short Questions

Here are some short **Yes/ No** questions

Answer them and write a short **justification** of your answer

Q1 $2^{\{1,2\}} \cap \{1, 2\} \neq \emptyset$

Q2 $\{\{a, b\}\} \in 2^{\{a,b,\{a,b\}\}}$

Q3 $\emptyset \in 2^{\{a,b,\{a,b\}\}}$

Q4 Any function f from $A \neq \emptyset$ onto A, has property

$f(a) \neq a$ for certain $a \in A$

Simple Short Questions

Q5 Let $f: N \longrightarrow \mathcal{P}(N)$ be given by a formula:

$$f(n) = \{m \in N : \quad m < n^2\}$$

then $\emptyset \in f[\{0, 1, 2\}]$

Q6 Some relations

$$R \subseteq A \times B$$

are functions that map the set A into the set B

Answers to Short Questions

Q1 $2^{\{1,2\}} \cap \{1,2\} \neq \emptyset$

NO because

$$2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\} \cap \{1,2\} = \emptyset$$

Q2 $\{\{a,b\}\} \in 2^{\{a,b,\{a,b\}\}}$

YES because

have that $\{a,b\} \subseteq \{a,b,\{a,b\}\}$ and hence

$$\{\{a,b\}\} \in 2^{\{a,b,\{a,b\}\}}$$

by definition of the set of all subsets of a given set

Answers to Short Questions

Q2 $\{\{a, b\}\} \in 2^{\{a,b,\{a,b\}\}}$

YES other solution

We **list** all subsets of the set $\{a, b, \{a, b\}\}$,

i.e. all **elements** of the set

$$2^{\{a,b,\{a,b\}\}}$$

We start as follows

$$\{\emptyset,\ \{a\},\ \{b\},\ \{\{a, b\}\},\ \ldots, \ldots\}$$

and observe that we can **stop** listing because we reached the set $\{\{a, b\}\}$

This proves that $\{\{a, b\}\} \in 2^{\{a,b,\{a,b\}\}}$

Answers to Short Questions

Q3 $\emptyset \in 2^{\{a,b,\{a,b\}\}}$

YES because for any set A, we have that $\emptyset \subseteq A$

Q4 Any function f from $A \neq \emptyset$ onto A has a property

$f(a) \neq a$ for certain $a \in A$

NO

Take a function such that $f(a) = a$ for all $a \in A$

Obviously f is "onto" and and **there is no** $a \in A$

for which $f(a) \neq a$

Answers to Short Questions

Q5 Let $f: N \longrightarrow \mathcal{P}(N)$ be given by formula:

$f(n) = \{m \in N : \ \ m < n^2\}$, then $\emptyset \in f[\{0,1,2\}]$

YES We evaluate

$f(0) = \{m \in N : \ \ m < 0\} = \emptyset$

$f(1) = \{m \in N : \ \ m < 1\} = \{0\}$

$f(2) = \{m \in N : \ \ m < 2^2\} = \{0,1,2,3\}$

and so by definition of $f[A]$ get that

$f[\{0,1,2\}] = \{\emptyset, \{0\}, \{0,1,2,3\}\}$ and hence $\emptyset \in f[\{0,1,2\}]$

Q6 Some $R \subseteq A \times B$ are functions that map A into B

YES: Functions are special type of relations

Simple Short Questions

Q7 $\{(1,2),(a,1)\}$ is a binary relation on $\{1,2\}$

Q8 For any binary relation $R \subseteq A \times A$, the **inverse** relation R^{-1} **exists**

Q9 For any **binary relation** $R \subseteq A \times A$ that is a function, the **inverse function** R^{-1} exists

Simple Short Questions

Q10 Let $A = \{a, \{a\}, \emptyset\}$ and $B = \{\emptyset, \{\emptyset\}, \emptyset\}$
there is a function $f : A \xrightarrow[onto]{1-1} B$

Q11 Let $f : A \longrightarrow B$ and $g : B \xrightarrow{onto} A$,
then the **compositions** $(g \circ f)$ and $(f \circ g)$ **exist**

Q12 The function $f : N \longrightarrow \mathcal{P}(R)$ given by the formula:

$$f(n) = \{x \in R : \ x > \frac{ln(n^3 + 1)}{\sqrt{n + 6}}\}$$

is a **sequence**

Answers to Short Questions

Q7 $\{(1,2),(a,1)\}$ is a binary relation on $\{1,2\}$

NO because $(a,1) \notin \{1,2\} \times \{1,2\}$

Q8 For any binary relation $R \subseteq A \times A$, the inverse relation R^{-1} **exists**

YES By definition, the **inverse relation** to $R \subseteq A \times A$ is the set

$$R^{-1} = \{(b,a) : \quad (a,b) \in R\}$$

and it is a **well defined** relation in the set A

Answers to Short Questions

Q9 For any **binary relation** $R \subseteq A \times A$ that is a function, the **inverse function** R^{-1} exists

NO R must be also a 1 – 1 and *onto* function

Q10 Let $A = \{a, \{a\}, \emptyset\}$ and $B = \{\emptyset, \{\emptyset\}, \emptyset\}$

there is a function $f : A \xrightarrow[onto]{1-1} B$

NO The set A has **3** elements and the set

$$B = \{\emptyset, \{\emptyset\}, \emptyset\} = \{\emptyset, \{\emptyset\}\}$$

has **2** elements and an onto function does not exists

Answers to Short Questions

Q11 Let $f: A \longrightarrow B$ and $g: B \longrightarrow^{onto} A$,
then the **compositions** $(g \circ f)$ and $(f \circ g)$ **exist**

YES The composition $(f \circ g)$ **exists** because the functions $f: A \longrightarrow \mathbf{B}$ and $g: \mathbf{B} \longrightarrow^{onto} A$ **share** the same set $\mathbf{B}$

The composition $(g \circ f)$ **exists** because the functions $g: B \longrightarrow^{onto} \mathbf{A}$ and $f: \mathbf{A} \longrightarrow B$ **share** the same set $\mathbf{A}$

The information "onto" is irrelevant

Answers to Short Questions

Q12 The function $f: N \longrightarrow \mathcal{P}(R)$ given by the formula:

$$f(n) = \{x \in R : \quad x > \frac{ln(n^3 + 1)}{\sqrt{n+6}}\}$$

is a **sequence**

YES It is a sequence as the **domain** of the function f is the set N of natural numbers and the formula for f(n) assigns to each natural number n a certain **subset** of R, i.e. an **element** of $\mathcal{P}(R)$

CHAPTER 1

PART 3: Special Types of Binary Relations

Equivalence Relation

Equivalence relation

A binary relation $R \subseteq A \times A$ is an **equivalence** relation defined in the set A if and only if it is reflexive, symmetric and transitive

Symbols

We denote equivalence relation by symbols

$$\sim, \quad \approx \quad \text{or} \quad \equiv$$

We will use the symbol $\approx$ to denote the equivalence relation

Equivalence Relation

Equivalence class

Let $\approx \subseteq A \times A$ be an **equivalence** relation on A

The set

$$E(a) = \{b \in A : \quad a \approx b\}$$

is called an **equivalence class**

Symbol

The equivalence classes are usually **denoted** by

$$[a] = \{b \in A : \quad a \approx b\}$$

The element a is called a **representative** of the equivalence class $[a]$ defined in A

Partitions

Partition

A family of sets $\mathbf{P} \subseteq \mathcal{P}(A)$ is called a **partition** of the set A if and only if the following conditions hold

1. $\forall_{X \in \mathbf{P}} (X \neq \emptyset)$
   i.e. all sets in the partition are non-empty
2. $\forall_{X,Y \in \mathbf{P}} (X \cap Y = \emptyset)$
   i.e. all sets in the partition are disjoint
3. $\bigcup \mathbf{P} = A$
   i.e union of all sets from **P** is the set A

Equivalence and Partitions

Notation

$A/\approx$ denotes the set of **all equivalence** classes of the equivalence relation $\approx$, i.e.

$$A/\approx = \{[a] : a \in A\}$$

We prove the following theorem 1.3.1

Theorem 1

Let $A \neq \emptyset$

If $\approx$ is an **equivalence relation** on A,

then the set $A/\approx$ is a **partition** of A

Equivalence and Partitions

Theorem 1 (full statement)

Let $A \neq \emptyset$

If $\approx$ is an equivalence relation on A,

then the set $A/\approx$ is a **partition** of A, i.e.

1. $\forall_{[a]\in A/\approx} ([a] \neq \emptyset)$
   i.e. all equivalence classes are non-empty
2. $\forall_{[a]\neq[b]\in A/\approx} ([a] \cap [b] = \emptyset)$
   i.e. all different equivalence classes are disjoint
3. $\bigcup A/\approx = A$
   i.e the union of all equivalence classes is equal to the set A

Partition and Equivalence

We also prove a following

Theorem 2

For any **partition**

$$\mathbf{P} \subseteq \mathcal{P}(A) \quad \text{of the set} \quad A$$

one can **construct** a binary relation R on A such that R is an **equivalence** on A and its equivalence classes are exactly the sets of the **partition** **P**

Partition and Equivalence

Observe that we **can** consider, for any binary relation R on s set A the sets that "look" like equivalence classes i.e. that are defined as follows:

$$R(a) = \{b \in A; \;\; aRb\} = \{b \in A; \;\; (a, b) \in R\}$$

Fact 1

If the relation R is an **equivalence** on A, then the family $\{R(a)\}_{a \in A}$ is a **partition** of A

Fact 2

If the family $\{R(a)\}_{a \in A}$ is **not** a partition of A, then R is **not** an **equivalence** on A

Proof of Theorem 1

Theorem 1

Let $A \neq \emptyset$

If $\approx$ is an **equivalence relation** on A,

then the set $A/\approx$ is a **partition** of A

Proof

Let $A/\approx\; = \{[a] : a \in A\} = \mathbf{P}$

We must show that all sets in $\mathbf{P}$ are nonempty, disjoint, and together exhaust the set A

Proof of Theorem 1

1. All equivalence classes are nonempty,

This holds as $a \in [a]$ for all $a \in A$, reflexivity of equivalence relation

2. All different equivalence classes are disjoint

Consider two different equivalence classes $[a] \neq [b]$

Assume that $[a] \cap [b] \neq \emptyset$.

We have that $[a] \neq [b]$, thus there is an element c

such that $c \in [a]$ and $c \in [b]$

Hence $(a, c) \in \approx$ and $(c, b) \in \approx$

Since $\approx$ is **transitive**, we get $(a, b) \in \approx$

Proof of Theorem 1

Since $\approx$ is **symmetric**, we have that also $(a, b) \in \approx$

Now take any element $d \in [a]$;

then $(d, a) \in \approx$, and by **transitivity**, $(d, b) \in \approx$

Hence $d \in [b]$, so that $[a] \subseteq [b]$

Likewise $[b] \subseteq [a]$ and $[a] = [b]$ what contradicts the assumption that $[a] \neq [b]$

Proof of Theorem 1

3. To prove that

$$\bigcup A/\approx = \bigcup \mathbf{P} = A$$

we simply notice that each element $a \in A$ is in some set in $\mathbf{P}$

Namely we have by reflexivity that always

$$a \in [a]$$

This **ends** the proof of **Theorem 1**

Proof of the Theorem 2

Now we are going to prove that the **Theorem 1** can be reversed, namely that the following is also true

Theorem 2

For any **partition**

$$\mathbf{P} \subseteq \mathcal{P}(A)$$

of A, one can **construct** a binary relation R on A such that R is an **equivalence** and its equivalence classes are exactly the sets of the **partition** $\mathbf{P}$

Proof

We define a binary relation R as follows

$$R = \{(a, b) : \quad a, b \in X \text{ for some } X \in \mathbf{P}\}$$

Chapter 1

Some Short Questions

Short Questions

Q1 Let $R \subseteq A \times A$ for $A \neq \emptyset$, then the set

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

is an equivalence class with a **representative** a

Q2 The set

$$\{(\emptyset, \emptyset), (\{a\}, \{a\}), (3, 3)\}$$

represents a **transitive** relation

Short Questions

Q3 There is an **equivalence** relation on the set

$$A = \{\{0\}, \{0, 1\}, 1, 2\}$$

with **3** equivalence classes

Q4 Let $A \neq \emptyset$ be such that there are exactly **25 partitions** of A

It is possible to define **20 equivalence** relations on A

Short Questions Answers

Q1 Let $R \subseteq A \times A$ then the set

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

is an **equivalence** class with a **representative** a

NO The set $[a] = \{b \in A : (a, b) \in R\}$ is an equivalence class only when the relation R is an **equivalence** relation

Q2 The set

$$\{(\emptyset, \emptyset), (\{a\}, \{a\}), (3, 3)\}$$

represents a **transitive** relation

YES Transitivity condition is vacuously **true**

Short Questions Answers

Q3 There is an equivalence relation on

$$A = \{\{0\}, \{0,1\}, 1, 2\}$$

with **3** equivalence classes

YES For example, a relation R defined by the partition

$$\mathbf{P} = \{\{\{0\}\}, \ \{\{0,1\}\}, \ \{1,2\}\}$$

and so By proof of **Theorem 2**

$$R = \{(a,b): \ a,b \in X \text{ for some } X \in \mathbf{P}\}$$

i.e. $a = b = \{0\}$ or $a = b = \{0,1\}$ or ($a = 1$ and $b = 2$)

Short Questions Answers

Q4

Let $A \neq \emptyset$ be such that there are exactly **25** partitions of A
It is possible to define **2** equivalence relations on A

YES By **Theorem 2** one can define up to 25 (as many as partitions) of equivalence classes

Chapter 1

Some Long Questions

Long Questions

Q1 Consider a function $f: A \longrightarrow B$

Show that $R = \{(a, b) \in A \times A : f(a) = f(b)\}$

is an **equivalence** relation on A

Q2 Let $f: N \longrightarrow N$ be such that

$$f(n) = \begin{cases} 1 & \text{if } n \leq 6 \\ 2 & \text{if } n > 6 \end{cases}$$

Find equivalence classes of R from **Q1** for this particular function f

Long Questions Solutions

Q1 Consider a function $f: A \longrightarrow B$

Show that

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

is an **equivalence** relation on A

Solution

1. R is **reflexive**

$(a, a) \in R$ for all $a \in A$ because $f(a) = f(a)$

Long Questions Solutions

2. R is **symmetric**

Let $(a, b) \in R$, by definition $f(a) = f(b)$ and $f(b) = f(a)$

Consequently $(b, a) \in R$

3. R is **transitive**

For any $a, b, c \in A$ we get that $f(a) = f(b)$ and $f(b) = f(c)$

implies that $f(a) = f(c)$

Long Questions Solutions

Q2 Let $f: N \longrightarrow N$ be such that

$$f(n) = \begin{cases} 1 & \text{if } n \leq 6 \\ 2 & \text{if } n > 6 \end{cases}$$

Find **equivalence classes** of

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

for this particular f

Solution

We evaluate

$$[0] = \{n \in N: \ f(0) = f(n)\} = \{n \in N: \ f(n) = 1\}$$
$$= \{n \in N: \ n \leq 6\}$$

$$[7] = \{n \in N: \ f(7) = f(n)\} = \{n \in N: \ f(n) = 2\}$$
$$= \{n \in N: \ n > 6\}$$

There are **two** equivalence classes:

$$A_1 = \{n \in N: \ n \leq 6\}, \quad A_2 = \{n \in N: \ n > 6\}$$

Chapter 1

Order Relations

Order Relations

We introduce now of another type of important binary relations: the order relations

Definition

$R \subseteq A \times A$ is an order relation on A iff R is 1.Reflexive, 2. Antisymmetric, and 3. Transitive, i.e. the following conditions are satisfied

1. $\forall_{a \in A}(a, a) \in R$
2. $\forall_{a,b \in A}((a, b) \in R \cap (b, a) \in R \Rightarrow a = b)$
3. $\forall_{a,b,c \in A} ((a, b) \in R \cap (b, c) \in R \Rightarrow (a, c) \in R)$

Order Relations

Definition

$R \subseteq (A \times A)$ is a total order on A iff R is an order and any two elements of A are comparable, i.e. additionally the following condition is satisfied

4. $\forall_{a,b} \in A \ ((a,b) \in R \cup (b,a) \in R)$

Names: order relation is also called historically a partial order

total order is also called historically a linear order

Order Relations

Notations

order relations are usually denoted by $\leq$, or when we want to make a clear distinction from the natural order in sets of numbers we denote it by $\preceq$

Remember, that even if we use $\leq$ as the order relation symbol, it is a SYMBOL for ANY order relation and not only a symbol for a natural order $\leq$ in sets of numbers

Posets

A set $A \neq \emptyset$ ordered by an order relation R is called a poset

We write it as a tuple (depending of sumbols used)

(A, R), $(A, \leq)$, $(A, \preceq)$

Name poset stands historically for "partially ordered set".

Diagram of order relation is a graphical representation of a poset

It is a simplified graph constructed as follows.

1. As the order relation is reflexive, i.e. $(a, a) \in R$ for all $a \in A$, we draw a point with symbol a instead of a point with symbol a and the loop

2. As the order relation is antisymmetric we draw a point b **above** point a (connected, but without the arrow) to indicate that $(a, b) \in R$.

3. As the order relation in transitive, we connect points a, b, c without arrows

Posets Special Elements

Special elements in a poset $(A, \leq)$ are: maximal, minimal, greatest (largest) and smallest (least) and are defined below.

Smallest (least) $a_0 \in A$ is a smallest (least) element in the poset $(A, \leq)$ iff $\forall_{a \in A}(a_0 \leq a)$

Greatest (largest) $a_0 \in A$ is a greatest (largest) element in the poset $(A, \leq)$ iff $\forall_{a \in A}(a \leq a_0)$

Posets Special Elements

Maximal (formal) $a_0 \in A$ is a maximal element in the poset $(A, \leq)$ iff $\neg \exists_{a \in A}(a_0 \leq a \cap a_0 \neq a)$

Maximal (informal) $a_0 \in A$ is a maximal element in the poset $(A, \leq)$ iff on a diagram of $(A, \leq)$ there is no element placed above a_0

Minimal (formal) $a_0 \in A$ is a minimal element in the poset $(A, \leq)$ iff $\neg \exists_{a \in A}(a \leq a_0 \cap a_0 \neq a)$

Minimal (informal) $a_0 \in A$ is a minimal element in the poset $(A, \leq)$ iff on the diagram of $(A, \leq)$ there is no element placed below a_0

Some Properties of Posets

Use Mathematical Induction to prove the following property of finite posets

Property 1 Every non-empty finite poset has at least one maximal element

Proof

Let $(A, \leq)$ be a finite, not empty poset (partially ordered set by $\leq$, such that A has n-elements, i.e. $|A| = n$

We carry the Mathematical Induction over $n \in N - \{0\}$

Reminder: an element $a_o \in A$ ia a maximal element in a poset $(A, \leq)$ iff the following is true.

$$\neg \exists_{a \in A} (a_0 \neq a \cap a_0 \leq a)$$

Inductive Proof

Base case: $n = 1$, so $A = \{a\}$ and a is maximal (and minimal, and smallest, and largest) in the poset $(\{a\}, \leq)$

Inductive step: Assume that any set A such that $|A| = n$ has a maximal element;

Denote by a_0 the maximal element in $(A, \leq)$

Let B be a set with $n + 1$ elements; i.e. we can write B as

$B = A \cup \{b_0\}$ for $b_0 \notin A$, for some A with n elements

Inductive Proof

By **Inductive Assumption** the poset $(A, \leq)$ has a maximal element a_0

To show that $(B, \leq)$ has a maximal element we need to consider 3 cases.

1. $b_0 \leq a_0$; in this case a_0 is also a maximal element in $(B, \leq)$

2. $a_0 \leq b_0$; in this case b_0 is a new maximal in $(B, \leq)$

3. a_0, b_0 are not compatible; in this case a_0 remains maximal in $(B, \leq)$

By Mathematical Induction we have proved that

$\forall_{n \in \in N - \{0\}} (|A| = n \Rightarrow$ A has a maximal element)

Some Properties of Posets

We just proved

Property 1 Every non-empty finite poset has at least one maximal element

Show that the **Property 1** is not true for an infinite set

Solution: Consider a poset $(Z, \leq)$, where Z is the set on integers and $\leq$ is a natural order on Z. Obviously no maximal element!

Exercise: Prove

Property 2 Every non-empty finite poset has at least one minimal element

Show that the **Property 2** is not true for an infinite set