cse581
COMPUTER SCIENCE FOUNDAMENTALS: THEORY

Professor Anita Wasilewska

Lecture 2

DISCRETE MATHEMATICS BASICS

Discrete Mathematics Basics

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

Discrete Mathematics Basics

PART 3: Special types of Binary Relations

SPECIAL RELATION: Equivalence Relation

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

Equivalence relation is denoted in literature by symbols

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

We will use the symbol $\approx$ to denote it

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** with a **representant** a

Observe that by symmetry of the **equivalence** relation we have that

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

This proves the following

Equivalence class Property

Equivalence class is **independent** from the choice of its representants

Equivalence Classes

Equivalence Class Symbol

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

The equivalence classes are usually **denoted** by

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

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. the **union** of all sets from $\mathbf{P}$ 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

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

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

We must show that all sets in **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

We carry the proof by contradiction. Assume $[a] \neq [b]$ and $[a] \cap [b] \neq \emptyset$, thus there is an element c

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

Hence $a \approx c$ and $c \approx b$, hence by transitivity $a \approx b$

and so $[a] = [b]$ what **contradicts** the assumption that $[a] \neq [b]$

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

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

Short Review

PART 3: Equivalence Relations - Short and Long 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

Equivalence Relations

Some Long Questions

Some 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

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

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:

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

Discrete Mathematics Basics

PART 3: Special types of Binary Relations

SPECIAL RELATIONS: 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 if and only if 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

We use $\leq$ as the **order** relation symbol, it is a **symbol** for any order relation, not a the **natural order** in sets of numbers, unless we say so

Posets

Definition

Given $A \neq \emptyset$ and an **order** relation defined on A

A tuple

$$(A, \leq)$$

is called a **poset**

Name **poset** stands historically for Partially Ordered Set

A **Diagram** of is a graphical representation of a poset and is defined as follows

Posets

A **Diagram** of a poset $(A, \leq)$ is a **simplified graph** constructed as follows

1. As the **order** relation $\leq$ 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 with the loop

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

3. As the order relation is transitive, we connect points a, b, c with lines between points a, b, c located above each other, but without arrows

Posets Special Elements

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

Definitions

1. Smallest (least)

$a_0 \in A$ is a smallest (least) element in the poset $(A, \leq)$ if and only if $\forall_{a \in A}(a_0 \leq a)$

2. Greatest (largest)

$a_0 \in A$ is a greatest (largest) element in the poset $(A, \leq)$ if and only if $\forall_{a \in A}(a \leq a_0)$

Posets Special Elements

Definitions

3. Maximal (formal)

$a_0 \in A$ is a maximal element in the poset $(A, \leq)$

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

Maximal (informal)

$a_0 \in A$ is a maximal element in the poset $(A, \leq)$

if and only if on the diagram of $(A, \leq)$ there is **no element** placed **above** a_0

Posets Special Elements

Definitions

4. Minimal (formal)

$a_0 \in A$ is a minimal element in the poset $(A, \leq)$

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

Minimal (informal)

$a_0 \in A$ is a minimal element in the poset $(A, \leq)$

if and only if on the diagram of $(A, \leq)$ there is **no element** placed **below** a_0

Some Properties of Posets

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

Proof

Let $(A, \leq)$ be a finite, not empty poset with the set A such that $|A| = n$ for $n \in N - \{0\}$

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

Reminder: an element $a_o \in A$ is a **maximal element** in the poset $(A, \leq)$ if and only if

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

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 poset $(A, \leq)$ with n -elements has a maximal element $a_0 \in A$. We want to prove that any poset $(B, \leq)$ with $n + 1$ elements has at least one maximal element.

Consider $(B, \leq)$ with with $n + 1$ elements. Observe that we can always represent the set B as

$B = A \cup \{b\}$ for some $b \notin A$ and the set A has n elements

Inductive Proof

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

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

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

2. $a_0 \leq b$; in this case b is a maximal element in poset $(B, \leq)$

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

This end the proof

Some Properties of Posets

Exercise 1

We just proved the **Property 1** saying that every non-empty finite poset has at least one maximal element

Show an example an infinite poset $(A, \leq)$ in which **Property 1 does not** hold

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

Exercise 2

Give an example an infinite poset $(A, \leq)$ in which **Property 1 does hold** and $(A, \leq)$ has a unique maximal element

Solution: Consider a poset $(Z, \leq)$, where Z is the set on integers and $\leq$ is the natural order on $Z - \{0\}$ and $\leq$ is equality $=$ on the set $\{0\}$

Discrete Mathematics Basics

PART4: Lattices and Boolean Algebras

Upper Bound

Given a poset $(A, \preceq)$

$a_0 \in A$ is an **upper bound** of a non empty set $B \subseteq A$ if and only if

$\forall b \in B \ (b \preceq a_0)$

Lower Bound

Given a non empty poset $(A, \preceq)$

$a_0 \in A$ is a **lower bound** of a non empty set $B \subseteq A$ if and only if

$\forall b \in B \ (a_0 \preceq b)$

LATTICES

Greatest lower bound of B (glb B)

Given a poset $(A, \preceq)$

$b_0 \in A$ is a **greatest lower bound** of $B \subseteq A$ $(b_0 = glbB)$

if and only if b_0 is the **greatest** element the set **all lower bounds** of B

Least upper bound of B (lub B)

Given a poset $(A, \preceq)$ and a set $B \subseteq A$

$b_0 \in A$ is a **least upper bound** of B $(b_0 = lubB)$

if and only if b_0 is the **least** element of the set **all upper bounds** of B

LATTICE DEFINITION

Lattice

A poset $(A, \leq)$ is a **lattice** if and only if

for all $a, b \in A$, $lub\{a, b\}$ and $glb\{a, b\}$ **exist**

Lattice notation

We denote $lub\{a, b\} = a \cup b$ and $glb\{a, b\} = a \cap b$

The element $lub\{a, b\} = a \cup b$ is called a **lattice union** (meet) of a and b

The element $glb\{a, b\} = a \cap b$ is called a **lattice intersection** (joint) of a and b

LATTICE DEFINITION

Lattice as an Algebra

An abstract algebra $(A, \cup, \cap)$, where $\cup, \cap$ are two argument **operations** defined on A is called a **lattice** if and only if the following conditions hold

L1 $a \cup b = b \cup a$ and $a \cap b = b \cap a$

L2 $(a \cup b) \cup c = a \cup (b \cup c)$
and $(a \cap b) \cap c = a \cap (b \cap c)$

L3 $a \cap (a \cup b) = a$ and $a \cup (a \cap b) = a$

Lattice axioms

The conditions **L1- L3** are called lattice axioms

LATTICE ORDERINGS

Lattice orderings

Let the algebra $(A, \cup, \cap)$ be a lattice. The relations

$a \leq b$ if and only if $a \cup b = b$

$a \leq b$ if and only if $a \cap b = a$

are **order relations** in the lattice universe A

and are called lattice orderings

Lattice Poset

A poset $(A, \leq)$ is called a lattice poset

DISTRIBUTIVE LATTICE

Distributive lattice

A lattice $(A, \cup, \cap)$ is called a distributive lattice

if and only if

for all $a, b, c \in A$ the following conditions hold

$$\begin{array}{ll} \text{L4} & a \cup (b \cap c) = (a \cup b) \cap (a \cup c) \\ \text{L5} & a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \end{array}$$

Distributive lattice axioms

Conditions **L4 - L5** from above are called distributive lattice axioms

LATTICE UNIT and ZERO

Given a **lattice poset** $(A, \leq)$

The **greatest** element in $(A, \leq)$ (if exists) is denoted by 1 and is called a **lattice unit**

The **least** (smallest) element in $(A, \leq)$ (if exists) it is denoted by 0 and called a **lattice zero**

Lattice with unit and zero

If 0 (lattice zero) and 1 (lattice unit) exist we write the lattice as $(A, \cup, \cap, 0, 1)$ and call it a lattice with zero and unit

LATTICE UNIT AXIOMS

Lattice Unit Axioms

Let $(A, \cup, \cap)$ be a lattice

An element $x \in A$ is called a **lattice unit** if and only if

for all $a, b, c \in A$ the following conditions hold

$x \cap a = a$ and $x \cup a = x$

If such element $x \in A$ exists we denote it by 1 and we write

the **lattice unit axioms** as follows.

L6 $\quad 1 \cap a = a$

L7 $\quad 1 \cup a = 1$

LATTICE ZERO AXIOMS

Lattice Zero Axioms

Let $(A, \cup, \cap)$ be a lattice

An element $x \in A$ is called a **lattice zero** if and only if

for all $a, b, c \in A$ the following conditions hold

$x \cap a = x$ and $x \cup a = a$

If such element $x \in A$ exists we denote it by 0 and we write

the **lattice unit axioms** as follows.

L8 $\quad 0 \cap a = 0$

L9 $\quad 0 \cup a = a$

BOOLEAN ALGEBRA DEFINITION and AXIOMS

Boolean Algebra Definition

A **distributive lattice** $(A, \cup, \cap, 1, 0)$ with zero and unit, such that each element has a **complement** is called a Boolean Algebra

Boolean Algebra Axioms

A lattice $(A, \cup, \cap, 1, 0)$ is called a **Boolean Algebra** if and only if the operations $\cap, \cup$ satisfy axioms **L1 -L5**,

$0 \in A$ and $1 \in A$ satisfy axioms **L6 - L9** and each element $a \in A$ has a **complement** $-a \in A$, i.e. the following axiom holds

L10 For all $a \in A$ there exists $-a \in A$ such that

$a \cup -a = 1$ and $a \cap -a = 0$