

# Mathematical Foundations

# Set

- a **set** is a collection of objects (**elements**)
  - $\{a,b,c\}$
- finite vs infinite sets
- $\emptyset$  denotes the empty set
- enumeration
  - $\{2,3,5,7,11,13,17,19\}$
- general expression
  - $\{x \mid x \text{ is prime and } x \leq 20\}$

# Subset and Powerset

- $A \subseteq B$  ( $A$  is a subset of  $B$ )
- $U$  is the universal set
- the set of subsets of  $A$  is the **powerset** of  $A$ , denoted by  **$P(A)$**
- example
  - $A = \{a, b\}$
  - $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- Question: Given  $|A| = n$  what is  $|P(A)|$  ?

# Operations

- Union

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

- Intersection

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

- Complement

$$\overline{A} = \{x \mid x \notin A \text{ and } x \in U\}$$

# Properties of Sets

- Idempotent laws:

$$A \cup A = A, A \cap A = A$$

- Commutative laws:

$$A \cup B = B \cup A, A \cap B = B \cap A$$

- Associative laws:

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

- Absorption laws:

$$A \cup (A \cap B) = A, A \cap (A \cup B) = A$$

# Properties of Sets (cont.)

- Distributive laws:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

- Involution law:  $\overline{\overline{A}} = A$

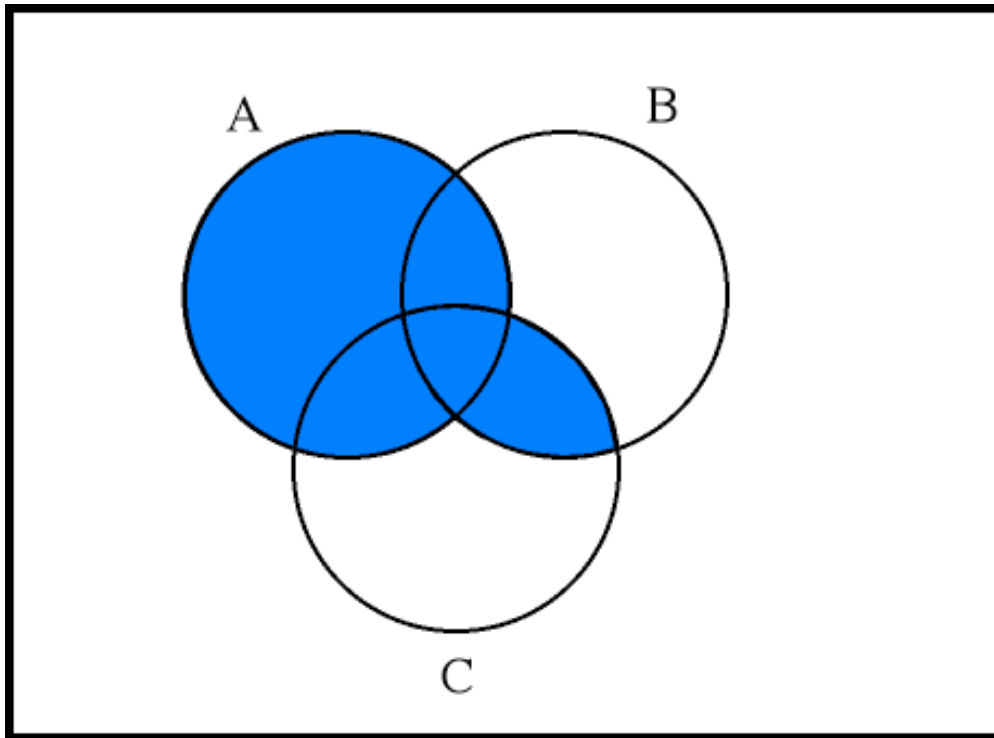
$$A \cup \overline{A} = U, A \cap \overline{A} = \emptyset;$$

$$A \cup \emptyset = A, A \cap U = A$$

$$A \cup U = U, A \cap \emptyset = \emptyset$$

- De Morgan's laws:  $\overline{(A \cup B)} = \overline{A} \cap \overline{B}, \overline{(A \cap B)} = \overline{A} \cup \overline{B}$

# Venn's Diagrams



$$A \cup (B \cap C)$$

# Relation

- a **tuple**  $(a,b)$  of two elements in a fixed order is an ordered **pair**
- **n-tuple**  $\implies$  tuple with  $n$  ordered elements
- direct product

- Example 
$$A \times B = \{(a,b) \mid a \in A, b \in B\}$$

let  $A = \{0, 1\}$  and  $B = \{0, 1, 2\}$

then,

$$A \times B = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$$

# Relation

- let  $A$  and  $B$  be sets
- and  $R \subseteq A \times B$
- $R$  is a binary relation
- inverse relation

$$R^{-1} = \{(b_j, a_i) \mid (a_i, b_j) \in R\}$$

- Example
- Let  $A = \{\text{John, Paul, Peter}\}$   
 $R = \text{“is father of”} = \{(\text{John, Paul}), (\text{Paul, Peter})\}$   
 $R^{-1} = \text{“is child of”} = \{(\text{Paul, John}), (\text{Peter, Paul})\}$

# Equivalence Class

- **Equivalence relation**
  1. reflective law:  $aRa$
  2. symmetric law: If  $aRb$ , then  $bRa$
  3. transitive law: If  $aRb$  and  $bRc$ , then  $aRc$

examples:

=

“have the same colour”

# Equivalence Class

- Let **R** be an equivalence relation on **A**
- we can partition **A** into blocks:  
$$[a] = \{x \mid aRx, x \in A\}$$
- **[a]** is an **equivalence class**
- **a** is a **representative** of **[a]**
- **A/R quotient set** (set of all equivalence classes)
- **rank** ==> number of equivalence classes

# Logic Notation

- let  $P$  and  $Q$  be **propositions**
- $P \Rightarrow Q$  “if  $P$  hold, then  $Q$  holds”
- $P \Leftrightarrow Q$  “ $P$  is true if and only if  $Q$  is true”
- $P \Rightarrow Q$

$P$  is a **sufficient** condition for  $Q$

$Q$  is a **necessary** condition for  $P$

- to prove  $P \Rightarrow Q$  is equivalent to prove the **contraposition**  $\overline{Q} \Rightarrow \overline{P}$

# Refinement

- if

$$xR_1y \Rightarrow xR_2y$$

- holds, then  $R_1$  is a refinement of  $R_2$ , and denoted by

$$R_1 \subseteq R_2$$

# Example

$A = \{011, 100, 110, 111\}$

$R_1$  “all corresponding bits are the same”

$R_2$  “the two rightmost bits are the same”

$R_3$  “the rightmost bits are the same”

011	100
111	110

$R_1$

011	100
111	110

$R_2$

011	100
111	110

$R_3$

$R_1 = \{(011,011), (100,100), (110,110), (111,111)\}$

$R_2 = \{(011,011), (100,100), (110,110), (111,111), (011,111), (111,011)\}$

$R_3 = \{(011,011), (100,100), (110,110), (111,111), (011,111), (111,011), (100,110), (110,100)\}$

# Functions

- if for each  $a \in A$ , there exists a unique element  $b \in B$  such that  $afb$ , then  $f$  is a **function** from  $A$  to  $B$  (or **mapping**)
- $f: A \rightarrow B$
- $A$  is the **domain**
- $f(a) = b$  is the **value** of the function  $f$  with respect to  $a$
- $b = f(a) \in B$  is an **image** of  $a \in A$
- $f(A) \subseteq B$  is the **range**

# Example

- $A = \{0, 1\}$ ,  $B = \{0, 1, 2\}$ ,  $C = \{0, 1, 2, 3, 4, 5, 6\}$
- $f: A \times B \times B \rightarrow C$
- $f(a, b, c) = a + b + c$

- Question:

What is the number of functions

$$f: A \times B \times B \rightarrow C$$

# Operations

- Unary and binary operations
- Example: let  $B=\{0,1\}$ . Let  $\bar{\phantom{a}}$  be a unary operation, and  $\wedge, \vee$ , and  $\oplus$  be binary operations

$$\bar{a} = 1 - a$$

$$a \wedge b = a \cdot b$$

$$a \vee b = a + b - a \cdot b$$

$$a \oplus b = a + b(\text{mod } 2)$$

# Ordered Relation

Partial ordered relation:

1. reflective law:  $aRa$
2. anti-symmetric law: If  $aRb$  and  $bRa$ , then  $a=b$
3. transitive law: If  $aRb$  and  $bRc$ , then  $aRc$

Total order relation

4. for all  $a, b \in A$ ,  $aRb$  or  $bRa$

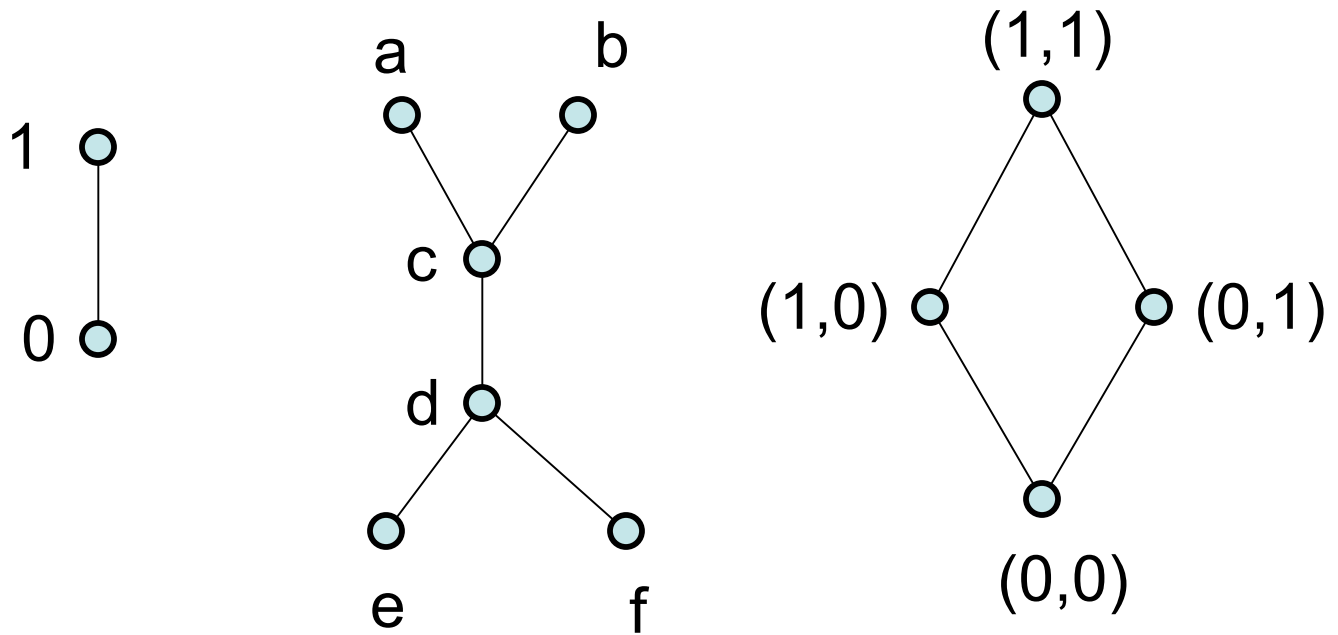
# Ordered Set

- Let  $\leq_R$  be an ordered relation defined on set  $A$ . A pair of  $A$  and  $\leq_R$ ,  $\langle A, \leq_R \rangle$ , is an **ordered set**.
- partial ordered set or total ordered set, depending on  $\leq_R$
- Example: Let  $P(A)$  be the powerset on  $A$ . Then  $\langle P(A), \subseteq \rangle$  is a partially ordered set.

# Hasse Diagram

- Let  $A$  be a finite set, and  $\leq_R$  be an ordered relation on  $A$ . Let  $a, b$ , be two elements in  $A$  such that  $a \leq_R b$  and  $a \neq b$ . If there is no element  $c$  such that  $a \leq_R c$ ,  $c \leq_R b$ , where  $c$  is different from  $a$  and  $b$ , then  $b$  **covers**  $a$ . When  $b$  covers  $a$ , the diagram which is obtained by writing  $b$  above  $a$ , and connecting it by a line.

# Hasse Diagrams



# Maximal/Minimal Element

- if there is no element  $a \in A$  such that  $a_0 \leq_R a$ , and  $a \neq a_0$ , then  $a_0$  is a **maximal element** of  $A$
- similarly **minimal element**
- **maximum element** - a unique maximal element

# LUB and GLB

- Let  $\langle A, \leq_R \rangle$  be an ordered set, and let  $B \subseteq A$ .  
The element  $a$  in  $A$  is an **upper bound** of  $B$ , if  $b \leq_R a$  for each element  $b$  in  $B$ .
- **least upper bound** - minimum upper bound
- similarly **lower bound** and **greatest lower bound**

# Questions

1. Let  $A$  and  $B$  be sets. How many binary relations are there?
2. Let  $N = \{1, 2, \dots, 10\}$ . Given the binary relation “have a common divisor”, draw the corresponding Hasse diagram.