Formal Method in Software Engineering (SE-313)

Course Teacher
Assistant Professor
Engr. Mustafa Latif

Set, Relations, and Functions

- **Sets are collections of well-defined objects;**
- **Relations indicate relationships between members of two sets A and B;**
- **Functions are a special type of relation where there is exactly (or at most) one relationship for each element a ε A with an element in B.**

Set, Relations, and Functions

- A set is a collection of well-defined(for a given value it is possible to determine whether or not it is a member of the set) objects that contains no duplicates.
- Examples of sets
  - The set of natural numbers $\mathbb{N}$, integer numbers $\mathbb{Z}$,rational numbers $\mathbb{Q}$.
- Venn diagrams may be used to represent sets pictorially.

3

Set, Relations, and Functions

- A binary relation R (A , B) where A and B are sets is a subset of the Cartesian product (A X B) of A and B.
- The domain of the relation is A, and the co-domain of the relation is B .
- The notation aRb signifies that there is a relation between a and b and that (a , b) $\in$ R.

4

Set, Relations, and Functions

- Functions may be total or partial.
- A total function $f: A \rightarrow B$ is a special relation such that for each element a ε A there is exactly one element $b \in B$. This is written as f(a) = b.
- A partial function differs from a total function in that the function may be undefined for one or more values of A.
- The domain of a function (denoted by dom f) is the set of values in A for which the partial function is defined.
- The domain of the function is A provided that f is a total function.
- The co-domain of the function is B.

5

Set Theory

- A set is a fundamental building block in mathematics, and it is defined as a collection of well-defined objects (same kind, distinct with no repetition)
- Most sets encountered in computer science are finite, as computers can only deal with finite entities.

6

Set Theory

- Example: The following are examples of sets.
  - The books on the shelves in a library;
  - The books those are currently overdue from the library;
  - The customers of a bank
  - The bank accounts in a bank;
  - The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$;
  - The integer numbers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$;
  - The non-negative integers $\mathbb{Z}+ = \{0, 1, 2, 3, \ldots\}$;
  - The set of prime numbers = {2, 3, 5, 7, 11, 13, 17, …};
  - The rational numbers are the set of quotients of integers. $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z} \text{ and } q \neq 0\}.$

7

Set Theory

- The order in which the elements are listed is not relevant; that is, the set {2, 4, 6, 8, 10} is the same as the set {8, 4, 2, 10, 6}.
- The use of a predicate allows a new set to be created from an existing set by using the predicate to restrict membership of the set.

8

Set Theory

- The set of even natural numbers may be defined by a predicate over the set of natural numbers that restricts membership to the even numbers. It is defined by: $\text{Evens} = \{x \mid x \in \mathbb{N} \wedge even(x)\}.$
- In this example, even(x) is a predicate that is true if x is even and false otherwise.
- In general, $A = \{x \ \varepsilon \ E \mid P(x)\}$ denotes a set A formed from a set E using the predicate P to restrict membership of A to those elements of E for which the predicate is true.

9

Set Theory

- The elements of a finite set S are denoted by {x1, x2, … x_n}.
- The elements of a infinite set S are denoted by {x1, x2, …}.
- The expression x ∈ S denotes that the element x is a member of the set S
- The expression x ∉ S indicates that x is not a member of the set S.

10

Set Theory

- A set S is a subset of a set T (denoted $S \subseteq T$) if whenever $s \in S$ then $s \in T$, and in this case the set T is said to be a superset of S (denoted $T \supseteq S$).
- Two sets S and T are said to be equal if they contain identical elements; that is, $S = T$ if and only if $S \subseteq T$ and $T \subseteq S$.
- A set S is a proper subset of a set T (denoted $S \subset T$) if $S \subseteq T$ and $S \neq T$. That is, every element of S is an element of T, and there is at least one element in T that is not an element of S. In this case, T is a proper superset of S (denoted $T \supset S$).

11

Set Theory

- The empty set (denoted by $\emptyset$ or {}) represents the set that has no elements. Clearly, $\emptyset$ is a subset of every set.
- The singleton set containing just one element x is denoted by {x}, and clearly $x \in \{x\}$ and $x \neq \{x\}$. Clearly, $y \in \{x\}$ if and only if $x = y$.

Example 4.2

(i) $\{1, 2\} \subseteq \{1, 2, 3\}$;
(ii) $\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$;

12

Set Theory

- **The cardinality (or size) of a finite set S defines the number of elements present in the set. It is denoted by $|S|$. The cardinality of an infinite set S is written as $|S| = \infty$.**

Example 4.3

(i) Given $A = \{2, 4, 5, 8, 10\}$, then $|A| = 5$.
(ii) Given $A = \{x \in \mathbb{Z} : x^2 = 9\}$, then $|A| = 2$.
(iii) Given $A = \{x \in \mathbb{Z} : x^2 = -9\}$, then $|A| = 0$.

13

Set Theoretical Operations

- **These include the Cartesian product operation; the power set of a set; the set union operation; the set intersection operation; the set difference operation; and the symmetric difference operation.**

14

Set Theoretical Operations

- Cartesian Product
- The Cartesian product allows a new set to be created from existing sets. The Cartesian product of two sets *S* and *T* (denoted *S* x *T*) is the set of ordered pairs {(s, t) | s ∈ S, t ∈ T}. Clearly, *S* x *T* ≠ *T* x *S* and so the Cartesian product of two sets is not commutative.
- Two ordered pairs (s_1,t_1) and (s_2,t_2) are considered equal if and only if $s_1 = s_2$ and $t_1 = t_2$.

15

Set Theoretical Operations

- Cartesian Product
- The Cartesian product may be extended to that of *n* sets S_1, S_2, …, S_n. The Cartesian product $S_1 \times S_2 \times \ldots \times S_n$ is the set of ordered tuples $\{(s_1, s_2, \ldots, s_n) \mid s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n\}$.
- Two ordered n-tuples $(s_1, s_2, \ldots, s_n)$ and $(s_1', s_2', \ldots, s_n')$ are considered equal if and only if $s_1 = s_1', s_2 = s_2', \ldots, s_n = s_n'$.

16

Set Theoretical Operations

- Cartesian Product
- The Cartesian product may also be applied to a single set S to create ordered *n*-tuples of *S*; that is, $S^n = S \times S \times \ldots\ldots \times S$ (*n* times).

17

Set Theoretical Operations

- Union and Intersection Operations
- The union of two sets A and B is denoted by A ∪ B. It results in a set that contains all of the members of A and of B and is defined by:

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

18

Set Theoretical Operations

- Union and Intersection Operations
- For example, suppose A = {1, 2, 3} and B = {2, 3, 4}, then A ∪ B = {1, 2, 3, 4}.
- Set union is a commutative operation; that is, A∪B = B ∪ A.

19

Set Theoretical Operations

- Union and Intersection Operations
- The intersection of two sets A and B is denoted by A ∩ B. It results in a set containing the elements that A and B have in common and is defined by:

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

20

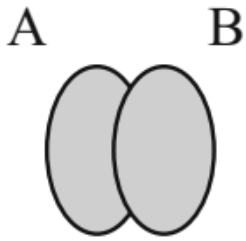
Set Theoretical Operations

- Union and Intersection Operations
- Suppose A = {1, 2, 3} and B = {2, 3, 4}, then A ∩ B = {2, 3}. Set intersection is a commutative operation; that is, A ∩ B = B ∩ A.
- Venn diagrams are used to illustrate these operations pictorially.

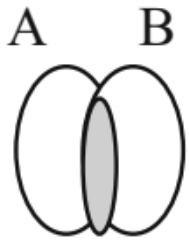
21

Set Theoretical Operations

- Union and Intersection Operations



$A \cup B$



$A \cap B$

22

Set Theoretical Operations

- Set Difference Operations
- The set difference operation A\B yields the elements in A that are not in B. It is defined by:

$$A \backslash B = \{a \mid a \in A \text{ and } a \notin B\}.$$

- For A and B defined as A = {1, 2} and B = {2, 3}, we have A\B = {1} and B\A = {3}. Clearly, set difference is not commutative; that is, A\B ≠ B\A.
- Clearly, A\A = ∅ and A\∅ = A.

23

Set Theoretical Operations

- Set Difference Operations
- The symmetric difference of two sets A and B is denoted by A Δ B and is given by:

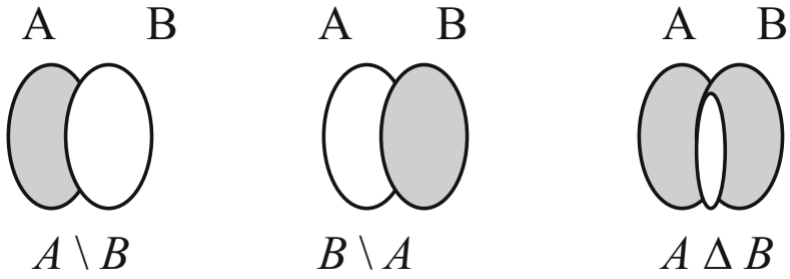
$$A \Delta B = A \backslash B \;\; B \backslash A$$

- The symmetric difference operation is commutative; that is, A Δ B = B Δ A.
- Venn diagrams are used to illustrate these operations pictorially.

24

Set Theoretical Operations

- **Set Difference Operations**



25

Set Theoretical Operations

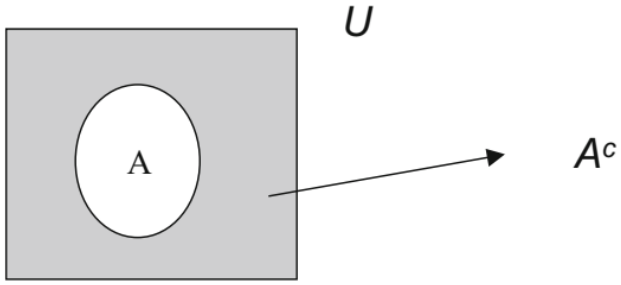
- **Complement of a set**
- **The complement of a set A (with respect to the universal set U) is the elements in the universal set that are not in A. It is denoted by A^c (or A') and is defined as:**

$$A^c = \{u | u \in U \text{ and } u \notin A\} = U \setminus A.$$

26

Set Theoretical Operations

- **Complement of a set**



- **The complement of the set A is illustrated by the shaded area above.**

27

Table 4.1 Properties of set operations

Property	Description
Commutative	Union and intersection operations are commutative; that is, $S \cup T = T \cup S$ $S \cup T = T \cap S$
Associative	Union and intersection operations are associative; that is, $R \cup (S \cup T) = (R \cup S) \cup T$ $R \cap (S \cap T) = (R \cap S) \cap T$
Identity	The identity under set union is the empty set $\varnothing$, and the identity under intersection is the universal set U $S \cup \emptyset = \emptyset \cup S = S$ $S \cap U = U \cap S = S$

28

Distributive	The union operator distributes over the intersection operator and vice versa $R \cap (S \cup T) = (R \cap S) \cup (R \cap T)$ $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$
De Morgan's[a] law	The complement of $S \cup T$ is given by: $(S \cup T)^c = S^c \cap T^c$ The complement of $S \cap T$ is given by: $(S \cap T)^c = S^c \cup T^c$

29

Relations

- **A binary relation R(A, B) where A and B are sets is a subset of A x B; that is, R ⊆ A x B. The domain of the relation is A, and the co-domain of the relation is B. The notation *aRb* signifies that (a, b) ∈ R.**
- **A binary relation *R(A, A)* is a relation between *A* and *A*. This type of relation may always be composed with itself, and its inverse is also a binary relation on *A*. The identity relation on *A* is defined by a i_Aa for all a ∈ A.**

30

Relations

There are many examples of relations:

- The relation on a set of students in a class where (a, b) ∈ R if the height of a is greater than the height of b
- The relation less than (<) between and ℝ and ℝ is given by:

$$\{(x, y) \in \mathbb{R}^2 \ : \ x < y\}$$

31

Relations

There are many examples of relations:

- A bank may represent the relationship between the set of accounts and the set of customers by a relation. The implementation of a bank account will often be a positive integer with at most eight decimal digits.
- The relationship between accounts and customers may be done with a relation R ⊆ A x B, with the set A chosen to be the set of natural numbers, and the set B chosen to be the set of all human beings alive or dead. The set A could also be chosen to be

$$A = \{n \in \mathbb{N}: n < 10^8\}$$

32

Relations

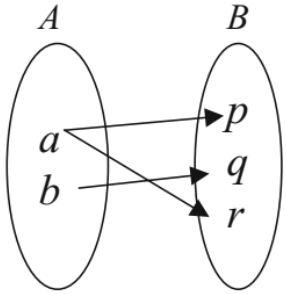
There are many examples of relations:

- A relation R(A, B) may be represented pictorially. An arrow from x to y is drawn if (x, y) is in the relation. Thus, for the height relation R given by {(a, p), (a, r), (b, q)}, an arrow is drawn from a to p, from a to r and from b to q to indicate that (a, p), (a, r) and (b, q) are in the relation R.

33

Relations

- The pictorial representation of the relation makes it easy to see that the height of a is greater than the height of p and r; and that the height of b is greater than the height of q.



34

Relations

Domain and Range of Relation

- The domain of a relation R (A, B) is given by $\{a \in A \mid \exists\, b \in B \text{ and } (a, b) \in R\}$. It is denoted by dom R.
  - The domain of the relation R = {(a, p), (a, r), (b, q)} is {a, b}.
- The range of a relation R (A, B) is given by $\{b \in B \mid \exists\, a \in A \text{ and } (a, b) \in R\}$. It is denoted by rng R.
  - The range of the relation R = {(a, p), (a, r), (b, q)} is {p, q, r}.

35

Relations

Inverse of a Relation

- Suppose $R \subseteq A \times B$ is a relation between A and B, then the inverse relation $R^{-1} \subseteq B \times A$ is defined as the relation between B and A and is given by:

$$b\, R^{-1}\ a \ \text{ if and only if } a\, R\, b.$$

$$R^{-1} = \{(b, a) \in B \times A : \ (a, b) \in R\}.$$

36

Relations

Composition of Relations

- The composition of two relations $R_1(A, B)$ and $R_2(B, C)$ is given by $R_2 \circ R_1$ where $(a, c) \in R_2 \circ R_1$ if and only there exists $b \in B$ such that $(a, b) \in R_1$ and $(b, c) \in R_2$. The composition of relations is associative; that is,

$$(R_3 \circ R_2) \circ R_1 = R_3 \circ (R_2 \circ R_1).$$

37

Relations

Composition of Relations

- Example: Consider a library that maintains two files. The first file maintains the serial number s of each book as well as the details of the author a of the book. This may be represented by the relation R_1 = sR1a. The second file maintains the library card number c of its borrowers and the serial number s of any books that they have borrowed. This may be represented by the relation R_2 = c R_2s.

38

Relations

Composition of Relations

- The library wishes to issue a reminder to its borrowers of the authors of all books currently on loan to them. This may be determined by the composition of $R_1 \circ R_2$, i.e. c $R_2 \circ R_1$ a if there is book with serial number s such that c R2 s and s R1 a.

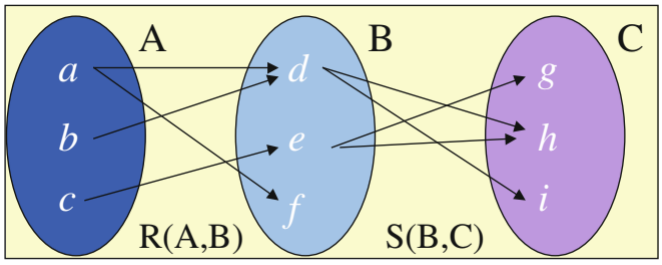
39

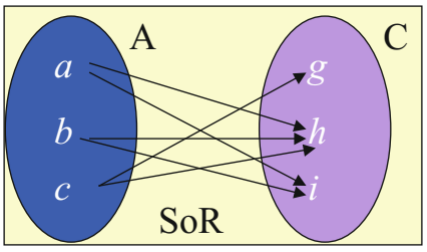
Relations

Composition of Relations

- Example: Consider sets A = {a, b, c}, B = {d, e, f}, C = {g, h, i} and relations R(A, B) = {(a, d), (a, f), (b, d), (c, e)} and S(B, C) = {(d, h), (d, i), (e, g), (e, h)}. Then, we graph these relations and show how to determine the composition pictorially.
- $S \circ R$ is determined by choosing $x \in A$ and $y \in C$ and checking if there is a route from x to y in the graph. If so, we join x to y in $S \circ R$.

40

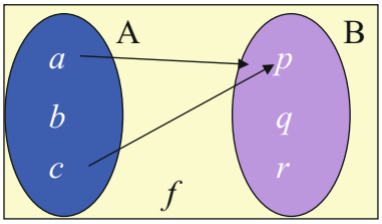




41

Functions

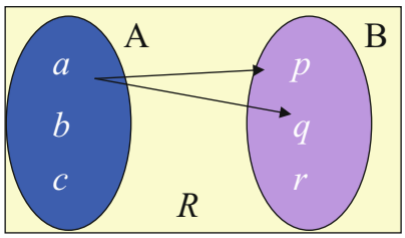
- A function f: A → B is a special relation such that for each element a ∈ A there is exactly (or at most) one element b ∈ B. This is written as f(a) = b.



42

Functions

- A function is a relation but not every relation is a function. For example, the relation in the diagram below is not a function since there are two arrows from the element a ∈ A.



43

Functions

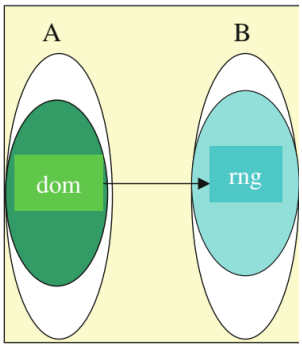
- The domain of the function (denoted by *dom* f) is the set of values in A for which the function is defined.
- The domain of the function is A provided that f is a total function.
- The co-domain of the function is B. The range of the function (denoted *rng* f) is a subset of the co-domain and consists of:

$$\mathbf{rng}\, f = \{r |\ r \in B \text{ such that } f(a) = r \text{ for some } a \in A\}.$$

44

Functions

- **Functions may be partial or total.**
- **A partial function (or partial mapping) may be undefined for some values of A, and partial functions arise regularly in the computing field (Fig. 4.9).**
- Total functions **are defined for every value in A, and many functions encountered in mathematics are total.**



45

Functions

- **Example: Functions are an essential part of mathematics and computer science, and there are many well-known functions such as the trigonometric functions sin(x), cos(x), and tan(x); the logarithmic function ln(x); the exponential functions e^x; and polynomial functions.**

46

Functions

- **Example:**

(i) Consider the partial function $f : \mathbb{R} \to \mathbb{R}$ where

$$f(x) = \frac{1}{x} \quad (\text{where } x \neq 0).$$

(ii) Consider the function $f : \mathbb{R} \to \mathbb{R}$ where

$$f(x) = x^2.$$

47

Functions

- **Example: Partial functions often arise in computing as a program may be undefined or fail to terminate for several values of its arguments (e.g. infinite loops). Care is required to ensure that the partial function is defined for the argument to which it is to be applied.**

48

Functions

- Example: Consider a program P that has one natural number as its input and which fails to terminate for some input values. It prints a single real result and halts when it terminates. Then, P can be regarded as a partial mapping from $\mathbb{N}$ to $\mathbb{R}$.

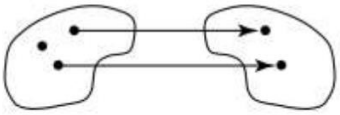
$$P : \mathbb{N} \rightarrow \mathbb{R}.$$

49

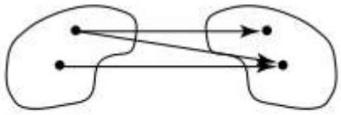
Functions

- Properties of function
- A function f: A → B is surjective (onto) if given any b ∈ B there exists an a ∈ A such that f(a) = b
- A function f: A ⟶ B is one-to-one or injecive if given any b ∈ B there exists a unique a ∈ A such that f(a) = b
- A function is bijective if it is one-to-one and onto

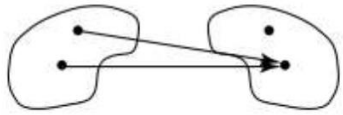
50



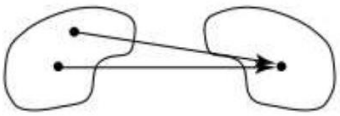
Not a Total function



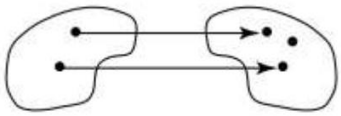
Not a function



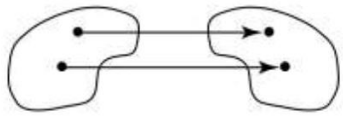
Function, not one-to-one, not onto



Function, not one-to-one, onto



Function, one-to-one, not onto



Function, one-to-one, onto

51

Functions

Inverse of function

- The relational inverse of the function may or may not be a function.
- However, if the relational inverse is a function, it is denoted by $f^{-1} : B \longrightarrow A$.
- A total function has an inverse (that is a total function) if and only if it is bijective,
- A partial function has an inverse if and only if it is injective.

52

Functions

Inverse of function

- The relational inverse of the function may or may not be a function.
- However, if the relational inverse is a function, it is denoted by $f^{-1} : B \longrightarrow A$.
- A total function has an inverse (that is a total function) if and only if it is bijective,
- A partial function has an inverse if and only if it is injective.