CS 5002: Discrete Structures **Fall 2018**

Lecture 6: October 11, 2018 [1]

Instructors: Tamara Bonaci, Adrienne Slaugther

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

Relations

Readings for this week:
Rosen, Chapter 9.1, 9.2, 9.3, 9.4, 9.5, 9.6

6.1 Overview

1. Review: number theory: divisibility, modular arithmetic, and congruences
2. Relations and their properties
3. Representing relations
4. Closures
5. Equivalence relations
6. Partial orderings
7. n-ary relations and their applications

6.2 Introduction

In today's lecture, we discuss the mathematics of relations defined on sets. **Relations** are a (data) structures typically used to represent various relationships between elements of sets. For example, in our everyday life, we recognize varous relationships, such as those between a person and their email address, a student and their grades, a country and its cities. We can use relations to represent those relationships, and solve some interesting problems on them. For example, determining which pairs of cities are linked by airline flights in a network, determining a viable sequence of courses to take to satisfy all of the degree requirements, etc.

Before we start talking about relations, however, let's go back, and briefly review the most important concepts from the last time.

6.3 Review

Last time, we introduce the notion of divisibility, and we said that, if a and b are integers such that $a \neq 0$, we say that **a divides b** if if there exist an integer c such that:

$$b = ac$$

or equivalently, $\frac{b}{a}$ is an integer. We introduce **the division algorithm** as follows.

Let a be some integer, and d some positive integer. Then there always exist unique integers q and r, where $0 \leq r < d$, such that:

$$a = dq + r \tag{6.1}$$

In equation (6.1), positive integer d is typically referred to as **divisor**, integer a as **dividend**, and integers q and r as **quotient** and **remainder**, respectively.

We next introduced **congruences**, and defined them as follows.

Let a and b be integers, $a, b \in \mathbb{Z}$ and let m be a positive integer, $m \in \mathbb{N}$. If m divides $(a - b)$, we can write:

$$a \equiv b \pmod{m}, \text{ or} \tag{6.2}$$

$$m|(a - b) \tag{6.3}$$

The operator $\equiv$ is called *congruence* and $a \equiv b \pmod{m}$ is read: "a **is congruent to** b **modulo** m." The positive integer m is known as the **modulus**.

We next defined **prime numbers** as those integers greater than one, whose only positive factors are 1 and p, and we answered the following questions about prime numbers:

- How do we show that some positive integer is a prime? **Trivial division**
- If an integer isn't a prime, how do we find all of its divisors (factors)? **Unique prime factorization**
- How many primes are there anyway? **Infinitely many**

We further introduced the concept of a **greatest common divisor** as follows:

Given two integers $a \neq 0$ and $b \neq 0$, the **greatest common divisor** of a and b (denoted $\gcd(a, b)$) is equal to the largest integer c that divides both a and b.

We defined that two integers $a \geq 1$ and $m \geq 2$ are said to be **relatively prime** or **coprime** if their greatest common divisor is equal to $gcd(a, m) = 1$.

We then answered the following questions?

- Given some positive integer a, how many integers from the set $\mathbb{Z}_a = \{1, 2, \ldots, a - 1\}$ are coprime with a? **Euler's totient function**
- How would we generally check whether or not two integers a and b are coprime? **Eucliedan algorithm**

We showed that fact that the greatest common divisor of some integers a and b can be expressed as a **linear combination of a and b**, and their corresponding linear coefficients

$$ax + by = d \tag{6.4}$$

where integers x and y are called **Bezout's coefficients**.

We further defined a **linear congruence** as a congruence of the form:

$$ax \equiv b \pmod{m}$$

where m is a positive integer, a and b are integers, and x is a variable, and we showed how and when can we solve such linear congruences.

To do so, we introduce the notion of a **modular multiplicative inverse** of an integer $a \in \mathbb{Z}_m$ modulo m, denoted as $a^{-1} \pmod{m}$, as an element $a' \in \mathbb{Z}_m$ such that:

$$a \cdot a' \equiv a' \cdot a \equiv 1 \pmod{m} \tag{6.5}$$

And we showed that, given the modular multiplicative inverse, some congruence $ax \equiv b \pmod{m}$ can be solved for x as follows:

$$\begin{aligned} ax &\equiv b \pmod{m} \\ \underbrace{a^{-1}(ax)}_{x} &\equiv a^{-1}(b) \pmod{m} \end{aligned}$$

We answered the following questions about modular multiplicative inverses:

- When does an integer $a \in \mathbb{Z}_m$ have a modular multiplicative inverse under modulo m?
- If an integer $a \in \mathbb{Z}_m$ have a modular multiplicative inverse under modulo m, how do we find it? **Extended Euclidean algorithm**

Theorem 6.1 (Fermat's Little Theorem) *Let's consider two integers a and p. If p is a prime, and p does not divide a, then:*

$$a^{p-1} = 1 \bmod p \tag{6.6}$$

6.4 Relations and Their Properties

> *Mathematics is the tool specifically suited for dealine with abstract concepts of any kind and there is no limit to its power in this field.* *P. A. M. Dirac (1902-1984)*

Relations are structures used to represent relationships between two or more sets. When a relation is defined between two sets, we talk about ***binary relations***, and when it is defined between more than two sets, we generally talk about ***n-ary relations*** (e.g., ternary, quaternary relations).

We formally define a binary relation as follows:

Definition 6.2 (Binary relation) *Let A and B be sets. A* **binary relation** *from A to B is a subset of a Cartesian product $A \times B$.*

In other words, a binary relation from A to B is a set R of ordered paris where the first element of each ordered pair comes from set A, and the second element comes from B.

Notation:

- aRb - pair $(a, b) \in R$
- $a \not{R} b$ - pair $(a, b) \notin R$

Let's see some examples:

Example 1: Let A be the set of people commuting daily across the 520 bridge in either direction (eastbound or westbound), and let B be the set of of tech companies with offices in Seattle, or on the Eastside. Let R be the relation that consists of pairs (a, b), where a is a person commuting daily over the bridge to go to work in company b.

For example, if John Smith commutes over the bridge to go to work in Amazon, in SLU, and Kristen Peters commutes over the bridge to go to work in Microsoft in Redmond, then pairs (John Smith, Amazon) and (Kristen Peters, Microsoft) belong to R.

Example 2: Let A be the cities around the world, and let B be the postal (ZIP) codes used all over the world. We can now define relation R by specifying that (a, b) belongs to R if a city a has a postal code b.

Example 3: Let's define a relation R from $\mathbb{R}$ to $\mathbb{R}$ as follows: for all real number x and y:

$$x \; R \; y \iff x < y$$

Are following pairs related by the given relation R?

(a) 69 R 5.5
(b) 22 R 37
(c) -226 R 0

Of special iterest to us are relations from some set A to itself, defined as follows:

Definition 6.3 (*Relation on a set*) *A* **a relation on a set** *A is a relation from set A to that same set A.*

Example 4 [A Relation on a Power Set]: Let $X = \{a, b, c\}$. The power set of X can be found as $\mathcal{P}(X) = \{(\emptyset), \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Let's now define a relation R from $\mathcal{P}(X)$ to $\mathcal{P}(X)$ as follows:

$$A \; R \; B \iff A \text{ has at least as many elements as B}$$

Are the following pairs related by R?

(a) $\{a, b\}$ and $\{b, c\}$? YES.

(b) $\{a\}$ and $\{a, b, c\}$? NO.

Example 5 [The Congruence Module 2 Relation]: Let's define a relation R from $\mathbb{Z}$ to $\mathbb{Z}$ as follows:

$$\text{For all } (m, n) \in \mathbb{Z} \times \mathbb{Z} : m \ R \ n \iff m - n \text{ is even}$$

List five integers that are related to 1 by R.

Solution: There are many such lists. One is:

- 1, because 1 - 1 = 0, and 0 is even.
- 3, because 3 - 1 = 2, and 2 is even.
- 5 because 5 - 1 = 4, and 4 is even.
- -1 because -1 - 1 = -2, and -2 is even.
- -3, because -3 - 1 = -4, and -4 is even.

6.4.1 Functions as Relations

Let's recall that a function f from a set A to a set B assigns exactly one element of B to each element of A. The graph of f is the set of ordered pairs (a, b) such that $f(a) = b$. Because the graph of f is a subset of $A \times B$, it is a relation from A to B.

Therefore, whereas a function represents a relation **where exactly one element of B is related to each element in A**, an arbitrary relation can be used to **express a one-to-many relationship between elements of two sets**.

It follows that **relations are generalization of graphs of functions; they can be used to express a much wider class of relationships between sets.**

6.4.2 Properties of Relations

There exist several important properties that we typically use to classify relations on a set. Let's define them here.

Definition 6.4 (***Reflexivity***) *A relation R on a set A is called* ***reflexive*** *if$(a, a) \in R$ for every element $a \in A$.*

Definition 6.5 (***Symmetry***) *A relation R on a set A is called* ***symmetric*** *if $(b, a) \in R$ whenever $(a, b) \in R$ for all $a, b \in A$.*

Definition 6.6 (***Anti-symmetry***) *A relation R on a set A is called* ***anti-symmetric*** *when it holds that for all $a, b \in A$ such that $(a, b) \in R$, if $(b, a) \in R$, then it follows that $a = b$.*

Note 1: A relation is called antisymmetric if and only if there are no pairs of distinct elements a and b with a related to b and b related to a. That is, the only way to have a related to b and b related to a is for a and b to be the same element.

Note 2: The definition of anti-symmetry implies that if for all $a, b \in A$ such that there exists $(a, b) \in R$, there doesn't exist a corresponding pair $(b, a) \in R$, then the implication `if (b, a) exists, then a= b` is vacuously true, and the given relation is **anti-symmetric**.

Additional example of an anti-symmetric relation:

- Let's consider the following relation on set $\{1, 2, 3, 4\}$, defined as:

  $$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$$

  The given relation includes all of the pairs of the form (a, a), but for every pair (a, b) where $a \neq b$, it does not contain its counterpart pair (b, a). That makes the given relation **anti-symmetric.**

Question 1: Are terms symmetric and antisymmetric opposites? No, because a relation can have both properties, or may lack both of them.

Some relations that are both symmetric and anti-symmetric:

- Empty relation
- Equality relation

Some relations that are neither symmetric and anti-symmetric:

- Preorder relation

Definition 6.7 (*Transitivity*) *A relation R on a set A is called **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.*

More informally, reflexivity, symmetry and transitivity properties say the following:

- **Reflexivity:** Each element of a set is related to itself.
- **Symmetry:** If any one element is related to any other element, then the second element is also related to the first.
- **Transitivity:** If any one element is related to a second, and that second element is related to some third element, then the first element is related to the third element too.

Let's see some examples:

Example 6: Let $A = \{0, 1, 2, 3\}$ and let's define relations R, S and T on A as follows:

1. $R = \{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (2, 2), (3, 0), (3, 3)\}$
2. $S = \{(0, 0), (0, 2), (0, 3), (2, 3)\}$
3. $T = \{(0, 1), (2, 3)\}$

Which of the given relations are reflexive, symmetric and/or transitive? Why?

Relation R: relation R is reflexive, symmetric, but not transitive.

- **Reflexive:** Each element in A is related to itself.
- **Symmetric:** Whenever one element in A is related by R to the second, then the second is related to the first too.

- **Not transitive:** There exist elements of A 0, 1 and 3 - such that $1 \ R \ 0$ and $0 \ R \ 3$, but not $1 \ R \ 3$.

Relation S: relation S is not reflexive and not symmetric, but it is transitive.

- **Not reflexive:** Element $(1,1) \not{i}nS$.
- **Not symmetric:** Pair $(0,2) \in S$, but $(2,0) \notin S$.
- **Transitive:** Whenever $(x,y) \in S$ and $(y,z) \in S$, then $(x,z) \in S$ too, for all $x,y,z \in \{0,1,2,3\}$.

Relation T: relation T is not reflexive and not symmetric, but it is transitive.

- **Not reflexive:** Element $(0,0) \not{i}nT$.
- **Not symmetric:** Pair $(0,1) \in T$, but $(1,0) \notin T$.
- **Not transitive:** For the given pairs, it does not hold that whenever $(x,y) \in T$ and $(y,z) \in T$, then $(x,z) \in T$ too, for all $x,y,z \in \{0,1,2,3\}$.

Summary:

- R is reflexive $\iff \forall x \in A, (x,x) \in R$
- S is symmetric $\iff \forall x,y \in A,$ if $(x,y) \in R,$ then $(y,x) \in R$
- R is transitive $\iff \forall x,y,z \in A,$ such that $(x,y) \in R$ and $(y,z) \in R$, then $(x,z) \in R$

6.4.3 Combining Relations

Since relations from A to B are a subset of a Cartesian product $A \times B$, two relations from A to B can be combined in any way two sets can be combined. Let's see some examples.

Example 7: Let $A = \{,1,3,5\}$ and $B = \{2,4,6,8\}$. The relations $R_1 = \{(1,2),(1,4),(1,6),(1,8)\}$ and $R_2 = \{(1,8),(3,2),(5,6)\}$ can be combined to obtain:

$$R_1 \cup R_2 = \{(1,2),(1,4),(1,6),(1,8),(3,2),(5,6)\}$$
$$R_1 \cap R_2 = \{(1,8)\}$$
$$R_1 - R_2 = \{(1,2),(1,4),(1,6)\}$$
$$R_2 - R_1 = \{(3,2),(5,6)\}$$

Definition 6.8 (Composite Relations) *Let R be a relation from a set A to a set B and S a relation from set B to set C. the composite relation of R and S is the relation consisting of ordered pairs (a,c), where $a \in A, c \in C$ and for which there exists an element $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$. We denote the composite of R and S by $S \circ R$.*

Example 8: Find the composite of relations R and S, where R is the relation from $\{0,2,4\}$ to $\{1,2,3,4\}$ with $R = \{(0,1),(2,1),(4,1)\}$, and S is the relation from $\{1,2,3,4\}$ to $\{5,6,7\}$, with $S = \{(1,5),(2,5),(3,5),(4,5)\}$.

Composite of relations R and S, $S \circ R$ is found using all ordered pairs from R and ordered pairs from S, where the second element of the ordered pair in R agrees with the first element of the ordered pair in S. For example, ordered pair (0, 1) in R and (1, 5) in S produce ordered pair $(0,5)$ in $S \circ R$.

So, following the similar procedure, we can find all the ordered pairs of the composite as follows: $S \circ R = \{(0,5),(2,5),(4,5)\}$.

Definition 6.9 (Composing a Relation with Itself) *Let R be a relation on the set A. The powers $R^n, n = 1, 2, 3, \dots$ are defined recursively as:*

$$R^1 = R, R^2 = R \circ R, \dots R^{n+1} = R^n \circ R$$

Example 9: Let R be a relation on the set A, defined as $R = \{(1,1),(1,3),(1,5)\}$. Find R^3.

Because R^2 $R \circ R$, we can find $R^2 = \{(1,1)\}$. Now, because $R^3 = R^2 \circ R$, we find again that $R^3 = \{(1,1)\}$.

6.5 Representing Relations

6.5.1 Representing Relations Using Matrices

A relation between some finite sets can be represented using **zero-one matrices**. Let's assume R is some relation from $A = \{a_1, a_2, \dots, a_m\}$ to $B = \{b_1, b_2, \dots, b_n\}$. Then this relation can be represented as a matrix $\mathbf{M}_R = [m_{ij}]$, defined as follows:

$$m_{ij} = \begin{cases} 1, (a_i, b_j) \in R \\ 0, (a_i, b_j) \notin R \end{cases}$$

In other words, the zero-one matrix representation has a 1 as its (i,j) entry when $(a_i, b_j) \in R$, and 0 as ts (i,j) entry when $(a_i, b_j) \notin R$. Let's see some examples.

Example 10: Suppose that $A = \{1,3,5\}$ and $B = \{1,2\}$. Let R be a relation from A to B containing (a,b) if $a \in A, b \in B$ and $a \geq b$. What is the matrix representation of R if $a_1 = 1, a_2 = 3, a_3 = 5, b_1 = 1$ and $b_2 = 2$.

The given relation is given as $R = \{(1,1),(3,1),(3,2),(5,1),(5,2)\}$. So, the matrix $\mathbf{M}_R$ is given as:

$$\mathbf{M}_R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Example 11: Suppose that a relation R on a set is represents by a matrix:

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Is R reflexive and symmetric?

Because all of the diagonal elements of the given matrix are equal to 1, the given relation is reflexive. Since the given matrix is not symmetric, the given relation is not symmetric.

6.6 Closures

Let's consider some general relation R on a set A. Such a relation may or may not have some property P, such as **reflexivity, symmetry or transitivity**.

If there now exists some other relation S with property P, that contains R such that S is a subset of every relation with property P conataining R, then S is called ***the closure*** of R with respect to property P.

Definition 6.10 (***Reflexive closure***) *Let A be a set and R a relation on A. The* **reflexive closure** *of R is the relation R^r on A that satisfies the following three properties:*

- *R^r is reflexive.*
- *$R \subseteq R^r$*
- *If S is any other reflexive relation that contains R, then $R^r \subseteq S$.*

Definition 6.11 (***Symmetric closure***) *Let A be a set and R a relation on A. The* **symmetric closure** *of R is the relation R^s on A that satisfies the following three properties:*

- *R^s is symmetric.*
- *$R \subseteq R^s$*
- *If S is any other symmetric relation that contains R, then $R^s \subseteq S$.*

Definition 6.12 (***Transitive closure***) *Let A be a set and R a relation on A. The* **transitive closure** *of R is the relation R^t on A that satisfies the following three properties:*

- *R^t is transitive.*
- *$R \subseteq R^t$*
- *If S is any other transitive relation that contains R, then $R^t \subseteq S$.*

6.7 Equivalence Relations

In many real life examples, we often need to relate objects that are similar in some ways. Luckily for us, thre exists relations with a particular combinations of properties that allow us to do exactly that. One such special group of relations are **equivalence relations**. Let's explore them next.

Definition 6.13 (***Equivalence relation***) *A relation on a set A is called an equivalence relation if it is reflexive, symmetric and transitive.*

Definition 6.14 *Two elements a and b that are related by an equivalence relation are called* ***equivalent****. We typically use notation $a \equiv b$ to denote that a and b are equivalent with respect to some relation R,*

Let's see some examples.

Example 12: Let X be the set of all non-empty subsets of $\{1, 2, 3\}$:

$$X = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Let's define relation R on X as follows: for all A and B in X,

$$A \ R \ B \leftrightarrow \text{ the least element of } A \text{ equals the least element of } B$$

Is R an equivalence relation on X?

Yes, the given relation is an equivalence relation. To show that, we need to show that R is reflexive, symmetric and transitive.

- R **is reflexive:** (we need to show that $A \ R \ A$) Suppose A is some non-empty subset of $\{1, 2, 3\}$. Which ever subset we take, its least element will be equal to itself. So, by definition, the given relation is reflexive.
- R **is symmetric:** Suppose A and B are some non-empty subsets of $\{1, 2, 3\}$ and $A R B$. We need to show that $B \ R \ A$. Since $A \ R \ B$, the least element of A is equal to the least element of B. By construction, the other side, that the least element of B is equal to the least element of A is also true. So, the given relation is symmetric.
- R **is transitive:** Suppose ,BA and C are some non-empty subsets of $\{1, 2, 3\}$, $A \ R \ B$, and $B \ R \ C$. We need to show that $A \ R \ C$. Since $A \ R \ B$, the least element of A is equal to the least element of B. Since $B \ R \ C$, the least element of B is equal to the least element of C. By construction, the least element of A is equal to the least element of C is also true. So, the given relation is transitive.

6.7.1 Equivalence Classes

Suppose there exist some equivalence relation on a certain set. If a is some particular element of the set, then one may ask: "What is the subset of all elements of the set that are related to a". Such a subset is tupically called an **equivalence class of** a, and it is defined as follows.

Definition 6.15 (***Equivalence Class***) *Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the* **equivalence class of** *a.*

Notation:

- The equivalence class of a with respect to R is typically denotes as $[a]_R$.
- If R is an equivalence relation on a set A, the equivalence class of the element a is $[a]_R = \{s|(a,s) \in R\}$.
- Element b such that $b \in [a]_R$ is typically called ***representative*** of the given equivalence class.

Example 13: Let $A = \{0,1,2,3,4\}$, and let's define a relation R on A as follows:

$$R = \{(0,0),(0,4),(1,1),(1,3),(2,2),(3,1),(3,3),(4,0),(4,4)\}$$

It can be shown that the given relation is an equivalence relation. Let's find the distinct equivalence classes of R.

$$[0] = \{x \in A|xR0\} = \{0,4\}$$
$$[1] = \{x \in A|xR1\} = \{1,3\}$$
$$[2] = \{x \in A|xR2\} = \{2\}$$
$$[3] = \{x \in A|xR3\} = \{1,3\}$$
$$[4] = \{x \in A|xR4\} = \{0,4\}$$

We can observe that $[0] = [4]$ and $[1] = [3]$. So the **distinct** equivalence classes of the given relation are $\{0,4\},\{1,3\},\{2\}$.

6.7.2 Equivalence Classes and Partitions

It is interesting to observe how equivalence classes of some equivalence relation partition a set into disjoint, non-empty susbsets. This leads to the notion of a **set partition**, a concept we introduce next.

Definition 6.16 (***Set Partition***) *A* **partition** *of some set A if a finite or an infonite collection of non-empty, mutually disjoint subsets whose union is A.*

Definition 6.17 (***Relation Induced by a Partition***) *Given a parition of a set A, the* **relation induced by the partition**, *R, is defined on A as follows: For all $x, y \in A$,*

$$x \ R \ y \leftrightarrow \textit{there is a subset } A_i \textit{ of the partition such that both } x \textit{ and } y \textit{ are in } A_i$$

Theorem 6.18 (Partition → Relation) *Let A be a set with a partition, and let R be the relation induced by the partition. Then R is an equivalenece relation.*

Theorem 6.19 (Relation → Partition) *Let A be a set, and r a n equivalenece relation on A. Then the distinct equivalence classes of R form a partition of A. That is, the union of the equivalence classes covers the whole A ,adn the intersection of any two distinct classes is an empty set.*

Theorems 6.19 and 6.18 can be combined into a single theorem as follows.

Theorem 6.20 *Let R be an equivalence relation on some set S. Then the equivalence classes of R form a partition of S. Conversly, given a partition $\{A_i | i \in I\}$ of the set S, there exists an equivalence relation R that has the set $A_i, i \in I$ as its equivalence relation.*

The given theorems now allows us to state the following theorem about equivalence relations on some set A.

Theorem 6.21 *Let R be an equivalence relation on a set A. Then these statements for some elements a and b of A are equivalent:*

(i) $a \ R \ b$
(ii) $[a] = [b]$
(iii) $[a] \cap [b] \neq \emptyset$

Let's see some examples.

Example 14: What are the sets in the partion of the integers arising from congruence modulo 5?

There exists five congruence classes, corresponding to $[0]_5, [1]_5, [2]_5, [3]_5$ and $[4]_5$. They are the sets:

$$\begin{aligned}
[0]_5 &= \{\dots, -10, -5, 0, 5, 10, \dots\} \\
[1]_5 &= \{\dots, -9, -4, 1, 6, 11, \dots\} \\
[2]_5 &= \{\dots, -8, -3, 2, 7, 12, \dots\} \\
[3]_5 &= \{\dots, -7, -2, 3, 8, 13, \dots\} \\
[4]_5 &= \{\dots, -6, -1, 4, 9, 14, \dots\}
\end{aligned}$$

These congruence clases are disjoint, and every integer is in exactly one of them. Therefore, these classes form a partition.

6.8 Partial Orderings

We often use relations to order some or all elements of sets. For example, we order words, using a relation containing pairs of words (x, y), where x combes before y in the dictionary. We similarly order the set of integers using the relation containing the pairs (x, y), where x is less than y.

Let's explore this concept of ordering elements of some set further, and let's start by defining a partial order as follows.

Definition 6.22 (***Partial ordering***) *A relation r on a set S is called a* **partial ordering** *or* **partial order** *if it is reflexive, antisymmetric and transitive. A set S, together with its partial ordering R is called a* **partially ordered set***, or* **poset***, and it is typically denoted as (S, R).*

Let's see some examples:

Example 15 (The subset relation): Let $\mathcal{A}$ be any collection of sets, and let's define the subset relation $\subseteq$ on $\mathcal{A}$ as follows:

$$\text{For every } U, V \in \mathcal{A}, U \subseteq V \leftrightarrow \text{ for all } x, \text{ if } x \in U, \text{ then } x \in V.$$

It can easily be shown that the given relation is reflexive and transitive. Show that it is anti-symmetric.

For $\subseteq$ to be anti-symmetric, it means that for all sets U and V in $\mathcal{A}$ if $U \subseteq V$ and $V \subseteq U$, then $U = V$. But that is true by the definition of equality of sets, so the given relation is anti-symmetric.

Example 16 (The "Less than or equal to" relation): Let S be a set of real numbers, and define the 'less than or equal to" relation $\leq$, on S as follows:

For all real numbers x and y in S:

$$x \leq y \leftrightarrow x < y \text{ or } x = y$$

Show that $\leq$ is a partial order relation.

- **$\leq$ is reflexive:** For $\leq$ to be reflexive means that $x \leq x$ for all real numbers $x \in S$. By definition of $\leq$, that is always true.
- *leq* **is anti-symmetric:** For $\leq$ to be anti-symmetric means that fro all real numbers x and $y \in S$, if $x \leq y$ and $y \leq x$, then $x = y$. This immediately follows from the definition of $\leq$.
- *leq* **is transitive**: For $\leq$ to be transitive means that for all real numbers x, y and $z \in S$, if $x \leq y$ and $y \leq z$, the $x \leq z$. This follows from the definition of $\leq$, and the transitivity property of order.

Given that $\leq$ is reflexive, anti-symmetric and transitive, it folows that it is the partial ordering relation.

In diffrent posets, we use different symbols, such as $\leq, \subseteq$ and — for partial ordering. However, we need a symbol that we can use when discussin the ordering relation of any arbitrary poset. We typically use notation $a \preceq b$ to denote that $(a, b) \in R$ is an arbitrary poset $(S, R)/$.

Definition 6.23 (***Comparable Elements***) *Some elements a and b of a poset $(s, \preceq)$ are called* **comparble** *if either $a \preceq b$ or $b \preceq b$. When a and b are elements of S such that neither $a \preceq b$ nor $b \preceq b$, a and b are called* **incomparable**.

The term **partial** is used to describe partial ordering because some pairs of elements may be incomparable. When every two elements in the set are comparable, the relation is called **total ordering**.

Definition 6.24 (***Chain***) *If $(S, \preceq)$ is a poset and every two elements of S are comparble, the S is called a* **totally order set**, *and $\preceq$ is called a* **total order** *or a* **linear order**. *A totally ordered set is also called a* **chain**.

Example 17: The poset $(Z, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever a and b are integers.

Definition 6.25 (***Well-ordered set***) *$(S, \preceq)$ is a* **well-ordered set** *if it is a poset such that $\preceq$ is a total ordering, and every non-empty subset of S has at least one element.*

6.8.1 Lexicographic Order

The words in a dictionary are linsted in alphabetical, or lexicographic order, which is based on the ordering of the letters in the alphabet. This is a special case of an ordering of strings on a set constructed from a partial ordering on a set. Let's see how that happens.

Theorem 6.26 *Let A be a set with a partial order relation R, and let S be a set of strings over A. Let's define a relation $\preceq$ on S as follows.*

For any two strings in S, $a_1 a_2 \ldots a_m$ and $b_1 b_2 \ldots b_m$ where m and n are positive integers:

1. *If $m \leq n$, and $a_i = b_i$ for all $i = 1, 2, \ldots, m$, then $a_1 a_2 \ldots a_m \preceq b_1 b_2 \ldots b_n$*
2. *For some integer k with $k \leq m \leq n$, and $k \geq 1$, $a_i = b_i$ for all $i = 1, 2, \ldots, k-1$, and $a_k \neq b_k$, but $a_k \ R \ b_k$, then $a_1 a_2 \ldots a_m \preceq b_1 b_2 \ldots b_n$*
3. *If ϵ is the null string and s is any string in S, then $\epsilon \preceq s$.*

If no strings are related other than by these three conditions, then $\preceq$ is a partial order relation.

Definition 6.27 (***Lexicographic Order***) *The partial order relation from theorem is called the* **lexicographic order** *for S that corresponds to the partial order R on A.*

6.9 n-ary Relations and Their Applications

Relationships among elements from more than two sets often arise in real life. Such relationship can be represented using ***n-ary relations***, defined as follows.

Definition 6.28 (n-ary Relations) *Let $A_1, A_2, \ldots, A_n$ be sets. An* ***n-ary relation*** *on these sets is a subset $A_1 \times A_2 \times \cdots \times A_n$. The sets $A_1, A_2, \ldots, A_n$ are called the* **domains** *of the relation, and n is called its* **degree**.

Example 19: Let R be a relation on $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ consisitng of quadruples (a, b, c, d), where a, b, c and d are integers such that $a > b > c > d$. Then $(5, 4, 3, 1) \in R$, but $(1, 2, 3, 4) \notin R$. The degree of this relation is 4, and its domains are equal to the set of integers.

Example 20: Let R be a relation consisting of a 4-tuple (ID_A, K_A, ID_B, K_B), representing a setup for a confidential communication between two entities, Alice and Bob. Here ID_A denotes the unique identity of Alice, K_A Alice's cryptographic secret, ID_B denotes the unique identity of Bob, K_B Bob's cryptographic secret.

6.9.1 Operations on n-ary Relations

There exists a variety of operations on n-ary relations, and those are especially useful to answer queries on databases that ask for an n-tuple that satisifies certain conditions (more about this in the next subsection).

The most basic operation on an n-art relations is determining all n-tuples in the $n-$ary relation that satisfy certain conditions. Let's see several such operations.

Definition 6.29 (Selection operator) *Let R be an n-ary relation and C a condition that elements in R must satisfy. Then the **selection operator** s_C maps the $n-$ary relation R to the $n-$ary relation of all $n-$tuples from R that satisfy the condition C.*

Definition 6.30 (Projection operator) *Let R be an n-ary relation. Then **projection** $P_{i_1 i_2 \ldots i_m}$ where $i_1 < i_2 < \cdots < i_m$ maps the $n-$tuple $(a_1, a_2, \ldots, a_n)$ to the $m-$tuple $(a_{i_1}, a_{i_2}, \ldots, a_{i_m})$.*

Projection operator is typically used to form a new n-ary relation by deleting the same fields in every record of the original relation.

Definition 6.31 (Join operator) *Let R be a relation of degree m and S a relation of degree n. The join $J_p(R, S)$ where $p \leq m$ and $p \leq n$ is a relation of degree $m + n - p$ that consists of all $(m + n - p)-$tuples $(a_1, a_2, \ldots, a_{m-p}, c_1, c_2), \ldots, c_p, b_1, b_2, \ldots, b_{n-p}$, where the $m-$tuple $(a_1, a_2, \ldots, a_{m-p}, c_1, c_2, \ldots, c_p)$ belongs to R, and the $n-$tuple $(c_1, c_2, \ldots, c_p, b_1, b_2, \ldots, b_{n-vp})$ belongs to S.*

The join operation is typically used to combine two tables into one when these table share some identical fields.