BLG501E – Discrete Mathematics

2021 – 2022 Fall Term

Asst. Prof. Gökhan SEÇİNTİ

Ordering / Order Relation

Strict Order

Partial Order

Total / Linear Order

Well-ordered Set

Lexicographic Order

Hasse Diagram

Induction and Transfinite Induction

Pigeonhole Principle

Ackermann Function

A Brief Reminder

- Properties of Relations
  - Reflexive Relations
  - Symmetric and Antisymmetric Relations
  - Transitive Relations

Reflexive Relations

Definition: R is *reflexive* iff $(a,a) \in R$ for every element $a \in A$.
Written symbolically, R is reflexive if and only if

$$\forall x[x \in U \longrightarrow (x,x) \in R]$$

Example: The following relations on the integers are reflexive:

$R_1 = \{(a,b) \mid a \leq b\}$,
$R_3 = \{(a,b) \mid a = b \text{ or } a = -b\}$,
$R_4 = \{(a,b) \mid a = b\}$.

The following relations are not reflexive:

$R_2 = \{(a,b) \mid a > b\}$ (note that $3 \ngtr 3$),
$R_5 = \{(a,b) \mid a = b + 1\}$ (note that $3 \neq 3 + 1$),
$R_6 = \{(a,b) \mid a + b \leq 3\}$ (note that $4 + 4 \nleq 3$).

If $A = \emptyset$ then the empty relation is reflexive vacuously. That is the empty relation on an empty set is reflexive!

Symmetric Relations

Definition: R is *symmetric* iff $(b,a) \in R$ whenever $(a,b) \in R$ for all $a,b \in A$. Written symbolically, R is symmetric if and only if

$$\forall x \forall y\, [(x,y) \in R \longrightarrow (y,x) \in R]$$

Example: The following relations on the integers are symmetric:

$R_3 = \{(a,b) \mid a = b \text{ or } a = -b\}$,
$R_4 = \{(a,b) \mid a = b\}$,
$R_6 = \{(a,b) \mid a + b \leq 3\}$.
The following are not symmetric:
$R_1 = \{(a,b) \mid a \leq b\}$ (note that $3 \leq 4$, but $4 \nleq 3$),
$R_2 = \{(a,b) \mid a > b\}$ (note that $4 > 3$, but $3 \ngtr 4$),
$R_5 = \{(a,b) \mid a = b + 1\}$ (note that $4 = 3 + 1$, but $3 \neq 4 + 1$).

Antisymmetric Relations

Definition:A relation R on a set A such that for all $a,b \in A$ if $(a,b) \in R$ and $(b,a) \in R$, then $a = b$ is called *antisymmetric*. Written symbolically, R is antisymmetric if and only if

$$\forall x \forall y\ [(x,y) \in R \land (y,x) \in R \longrightarrow x = y]$$

- **Example**: The following relations on the integers are antisymmetric:

  $R_1 = \{(a,b) \mid a \leq b\}$,
  $R_2 = \{(a,b) \mid a > b\}$,
  $R_4 = \{(a,b) \mid a = b\}$,
  $R_5 = \{(a,b) \mid a = b + 1\}$.

  For any integer, if a $a \leq b$ and $a \leq b$, then $a = b$.

  The following relations are not antisymmetric:

  $R_3 = \{(a,b) \mid a = b \text{ or } a = -b\}$
  (note that both $(1,-1)$ and $(-1,1)$ belong to R_3),
  $R_6 = \{(a,b) \mid a + b \leq 3\}$ (note that both $(1,2)$ and $(2,1)$ belong to R_6).

Transitive Relations

Definition: 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 $a,b,c \in A$. Written symbolically, R is transitive if and only if

$$\forall x \forall y \forall z[(x,y) \in R \land (y,z) \in R \longrightarrow (x,z) \in R]$$

- **Example**: The following relations on the integers are transitive:

  $R_1 = \{(a,b) \mid a \leq b\}$,

  For every integer, $a \leq b$ and $b \leq c$, then $b \leq c$.

  $R_2 = \{(a,b) \mid a > b\}$,

  $R_3 = \{(a,b) \mid a = b \text{ or } a = -b\}$,

  $R_4 = \{(a,b) \mid a = b\}$.

  The following are not transitive:

  $R_5 = \{(a,b) \mid a = b + 1\}$ (note that both (3,2) and (4,3) belong to R_5, but not (3,3)),

  $R_6 = \{(a,b) \mid a + b \leq 3\}$ (note that both (2,1) and (1,2) belong to R_6, but not (2,2)).

Strict, Quasi/Pre and Partial Orderings

Definition 1a: A relation *R* on a set S is called a ***strict ordering***, or *strict order*, if it is **irreflexive**, **asymmetric**, and **transitive**.

Definition 1b: A relation *R* on a set S is called a preorder or quasiorder is a binary relation that is **reflexive** and **transitive**. Preorders are more general than equivalence relations and (non-strict) partial orders, both of which are special cases of a preorder: an antisymmetric preorder is a partial order, and a symmetric preorder is an equivalence relation.

Definition 1c: A relation *R* on a set S is called a ***partial ordering***, or *partial order*, if it is **reflexive**, **antisymmetric**, and **transitive**. A set together with a partial ordering *R* is called a *partially ordered set*, or *poset*, and is denoted by (*S*, *R*). Members of *S* are called *elements* of the poset.

Strict, Quasi/Pre and Partial Orderings

	Reflexive	Symmetric	Transitive
Strict Order	Irreflexive	Asymmetric	Transitive
Quasi Order **Preorder**	Reflexive	Neither asymmetric nor antisymmetric	Transitive
Partial Order	Reflexive	Antisymmetric	Transitive

Partial Orderings (*continued*)

Example 1: Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.

- *Reflexivity*: $a \geq a$ for every integer a.
- *Antisymmetry*: If $a \geq b$ and $b \geq a$, then $a = b$.
- *Transitivity*: If $a \geq b$ and $b \geq c$, then $a \geq c$.

These properties all follow from the order axioms for the integers. (*See Appendix* 1).

Partial Orderings (*continued*)

Example 2: Show that the divisibility relation (|) is a partial ordering on the set of integers.

- *Reflexivity*: $a \mid a$ for all integers a. (*see Example* 9 *in Section* 9.1)
- *Antisymmetry*: If a and b are positive integers with $a \mid b$ and $b \mid a$, then $a = b$. (*see Example* 12 *in Section* 9.1)
- *Transitivity*: Suppose that a divides b and b divides c. Then there are positive integers k and l such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so a divides c. Therefore, the relation is transitive.

- $(\boldsymbol{Z}^+, \mid)$ is a poset.

Partial Orderings (*continued*)

Example 3a: Show that the inclusion relation ($\subseteq$) is a partial ordering on the power set of a set S.

- *Reflexivity*: $A \subseteq A$ whenever A is a subset of S.
- *Antisymmetry*: If $A \subseteq B$ and $B \subseteq A$, then $A = B$.
- *Transitivity*: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

The properties all follow from the definition of set inclusion.

Partial Orderings (*continued*)

Example 3b: Show that the types of ordering relations:

i) $P_i \rho P_j \Leftrightarrow |P_i| < \ |P_j|$

ii) $P_i \ll P_j \Leftrightarrow |P_i| \leq \ |P_j|$

ii) $P_i \subseteq P_j$ see Example 3a.

defined on the power set of a set *S*. $(P_i \in \wp(S))$

$$S = \{2,3,5,7\}$$

Power Set of S, $\wp(S)$ contains following:

$\{2,3,5,7\}$

$\{2,3,5\}$ $\{2,3,7\}$ $\{2,5,7\}$ $\{3,5,7\}$

$\{2,3\}$ **…** **…** **…** **…** $\{5,7\}$

$\{2\}$ $\{3\}$ $\{5\}$ $\{7\}$

$\{\}$

Comparability

Definition 2: The elements a and b of a poset $(S, \preccurlyeq)$ are *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$. When a and b are elements of S so that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, then a and b are called *incomparable*.

The symbol $\preccurlyeq$ is used to denote the relation in any poset.

Definition 3: If $(S, \preccurlyeq)$ is a poset and every two elements of S are comparable, S is called a ***totally ordered*** or ***linearly ordered set***, and $\preccurlyeq$ is called a *total order* or a *linear order.* A totally ordered set is also called a ***chain***.

Lexicographic Order

Definition: Given two posets $(A_1,\preccurlyeq_1)$ and $(A_2,\preccurlyeq_2)$, the *lexicographic ordering* on $A_1 \times A_2$ is defined by specifying that (a_1, a_2) is less than (b_1,b_2), that is,

$$(a_1, a_2) \prec (b_1,b_2),$$

either if $a_1 \prec_1 b_1$ or if $a_1 = b_1$ and $a_2 \prec_2 b_2$.

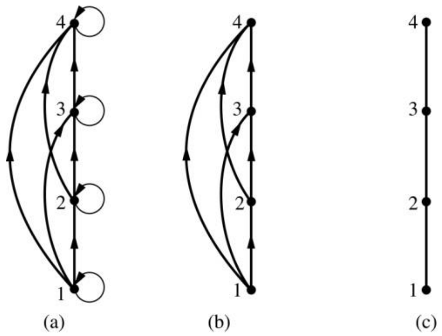
- This definition can be easily extended to a lexicographic ordering on strings (*see text*).

Example: Consider strings of lowercase English letters. A lexicographic ordering can be defined using the ordering of the letters in the alphabet. This is the same ordering as that used in dictionaries.

- *discreet* $\prec$ *discrete*, because these strings differ in the seventh position and $e \prec t$.
- *discreet* $\prec$ *discreetness*, because the first eight letters agree, but the second string is longer.

Hasse Diagrams

Definition: A *Hasse diagram* is a visual representation of a partial ordering that leaves out edges that must be present because of the reflexive and transitive properties.



A partial ordering is shown in (a) of the figure above. The loops due to the reflexive property are deleted in (b). The edges that must be present due to the transitive property are deleted in (c). The Hasse diagram for the partial ordering (a), is depicted in (c).

Procedure for Constructing a Hasse Diagram

- To represent a finite poset $(S, \preccurlyeq)$ using a Hasse diagram, start with the directed graph of the relation:
  - Remove the loops (a, a) present at every vertex due to the reflexive property.
  - Remove all edges (x, y) for which there is an element $z \in S$ such that $x \prec z$ and $z \prec y$. These are the edges that must be present due to the transitive property.
  - Arrange each edge so that its initial vertex is below the terminal vertex. Remove all the arrows, because all edges point upwards toward their terminal vertex.

Maximal and Minimal Elements

A poset $(E, \preccurlyeq)$ and $A \subseteq E$

- Minoran / lower bound

  $$\text{m} \in E \; is \; minoran(lowerbound) of A \Leftrightarrow \forall x \in A \Longrightarrow m \leq x$$

- Minimal

  $$\text{m} \in A \; is \; minimal \; of A \Leftrightarrow \forall x \in A \Longrightarrow \neg(x \leq m)$$

  There is no element in A such that x < m

- Minimum / least element

  If only one minimal element exists (unique)

Read: maximum of minoran set / greatest lower bound
minimum of majoran elements / least upper bound

Maximal and Minimal Elements

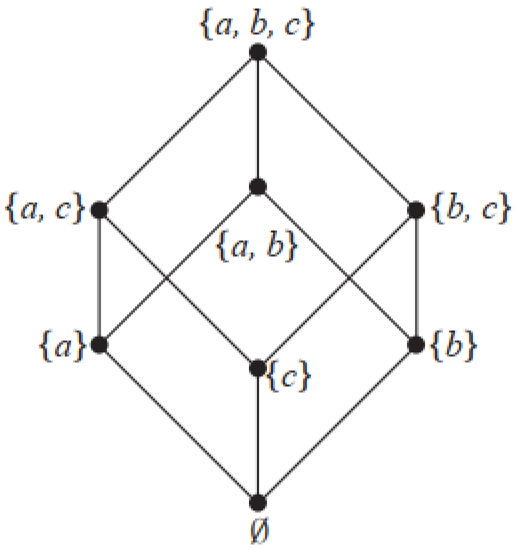


FIGURE 4 **The Hasse Diagram of $(P(\{a, b, c\}), \subseteq)$.**

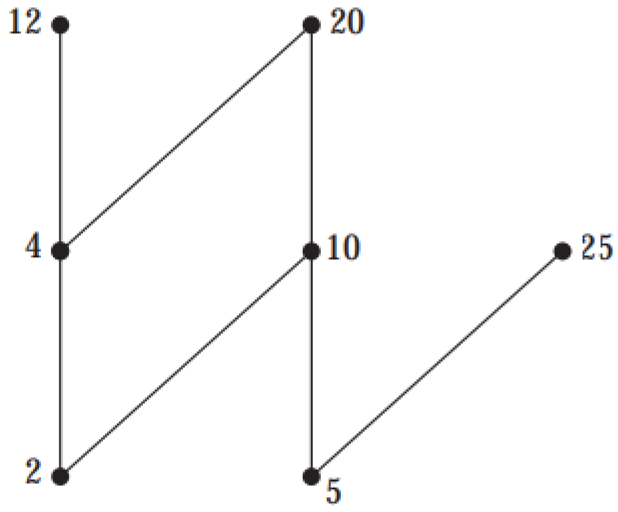


FIGURE 5 **The Hasse Diagram of a Poset.**

*Figures 4 and 5, Chapter 9

Well-ordered set and Noetherian ordered-set

Definition: (S,$\preccurlyeq$) is a **noetherian-ordered set** if it is a poset such that $\preccurlyeq$ every nonempty subset of S has at least one minimal element.

Definition 4: (S,$\preccurlyeq$) is a **well-ordered set** if it is a poset such that $\preccurlyeq$ is a total ordering and every nonempty subset of S has **a least element**.

Definition: Every Noetherian order with linear/total ordering property defines a well-order.

Mathematical Induction

For every well-ordered set in which every element has an preceding element.

i. Prove $P(0_{min})$

ii. $\forall x \in E,\ P(x) \Longrightarrow P(succ(x))$

In a lexicographic order
(0,n) → (0,n+1), but never reaches (1,0)

Example: Prove for $n \geq 4,\ 2^n < n!$

i. n=4, 16 < 4 3 2 ; 16 < 24

ii. n=k, $2^k < k!$

n = k+1 $2^{k+1} <?\, k+1!$

2 $2^k < k\ k!$; 2<k and $2^k < k!$

Transfinite Induction

Declerations:

LO: limit ordinals set (contains elements greater than minimal but without any predecessor)

M: minimal elements

(E, $\leq$) : Noetherian ordered set

i. $\forall 0_i \in M$; Prove $P(0_i)$

ii. $\forall x \in E,\ [\forall y \in \{y|\ y < x\}\, P(y)] \Rightarrow P(x)$

iii. $\forall x \in \mathrm{E}\ [\forall x \in LO \wedge \forall y \in \{y|y < x\}] \Rightarrow P(x)$

Transfinite Induction

Example:

Prove the following statement:

"Every natural number is a composite of prime numbers."

Proof of number *n*

$\forall k < n$ *assume the statement is TRUE.*
$k = a_1 a_2 \dots a_\varphi \wedge a_i \text{ is prime}.$

For n

Either n is prime then $n = n$

OR

n is not a prime, meaning that can be divided by other numbers. $n = u \cdot v$

BOTH u < n and v < n than $u = u_1 u_2 \dots u_\varphi$, $v = v_1 v_2 \dots v_\varphi$

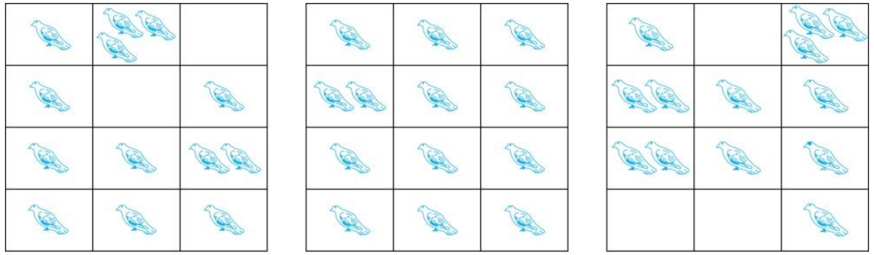
$n = u_1 u_2 \dots u_\varphi \, v_1 v_2 \dots v_\varphi \wedge u_i \text{and } v_i \text{are prime}.$

Dirichlet drawer principle

- The Pigeonhole Principle
- The Generalized Pigeonhole Principle

The Pigeonhole Principle

- If a flock of 20 pigeons roosts in a set of 19 pigeonholes, one of the pigeonholes must have more than 1 pigeon.



(a) (b) (c)

Pigeonhole Principle: If k is a positive integer and $k + 1$ objects are placed into k boxes, then at least one box contains two or more objects.

Proof: We use a proof by contraposition. Suppose none of the k boxes has more than one object. Then the total number of objects would be at most k. This contradicts the statement that we have $k + 1$ objects.

◀

The Pigeonhole Principle

Corollary 1: A function f from a set with $k + 1$ elements to a set with k elements is not one-to-one.

Proof: Use the pigeonhole principle.

- Create a box for each element y in the codomain of f .
- Put in the box for y all of the elements x from the domain such that $f(x) = y$.
- Because there are $k + 1$ elements and only k boxes, at least one box has two or more elements.

Hence, f can't be one-to-one.

◄

Pigeonhole Principle

Example: Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.

Example (*optional*): Show that for every integer *n* there is a multiple of *n* that has only 0s and 1s in its decimal expansion.

Solution: Let *n* be a positive integer. Consider the *n* + 1 integers 1, 11, 111, …., $11…1$ (where the last has *n* + 1 1s). There are *n* possible remainders when an integer is divided by *n*. By the pigeonhole principle, when each of the *n* + 1 integers is divided by *n*, at least two must have the same remainder. Subtract the smaller from the larger and the result is a multiple of *n* that has only 0s and 1s in its decimal expansion.

The Generalized Pigeonhole Principle

The Generalized Pigeonhole Principle: If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N/k \rceil$ objects.

Proof: We use a proof by contraposition. Suppose that none of the boxes contains more than $\lceil N/k \rceil - 1$ objects. Then the total number of objects is at most

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k} + 1\right) - 1\right) = N,$$

where the inequality $\lceil N/k \rceil < \lceil N/k \rceil + 1$ has been used. This is a contradiction because there are a total of n objects.

◀

Example: Among 100 people there are at least $\lceil 100/12 \rceil = 9$ who were born in the same month.

The Generalized Pigeonhole Principle

Example: a) How many cards must be selected from a standard deck of 52 cards to guarantee that at least three cards of the same suit are chosen?

b) How many must be selected to guarantee that at least three hearts are selected?

Solution: a) We assume four boxes; one for each suit. Using the generalized pigeonhole principle, at least one box contains at least $[N/4]$ cards. At least three cards of one suit are selected if $[N/4] \geq 3$. The smallest integer N such that $[N/4] \geq 3$ is $N = 2 \cdot 4 + 1 = 9$.

b) A deck contains 13 hearts and 39 cards which are not hearts. So, if we select 41 cards, we may have 39 cards which are not hearts along with 2 hearts. However, when we select 42 cards, we must have at least three hearts. (Note that the generalized pigeonhole principle is not used here.)

Dirichlet drawer principle

Example:

Declarations:

$$[2n] = \{1,2,3,4\ \ldots 2n-1,2n\}\ and\ |[2n]| = 2n$$
$$X_m \subseteq [2n] \wedge |X_m| = m \wedge m \geq n+1$$

Prove that

$$\exists p, q \in X_m \text{ such that } p = 2^a q \wedge a \in \mathrm{N}$$

Dirichlet drawer principle

Solution:

Part1: Proving $\forall x \in N^+, \exists! \, (r, y) \in NxN$

$$x = 2^r y \wedge y = 2p + 1 \wedge p \in N \wedge y \leq x$$

Using transfinite induction

Assume $\forall m \in \{m \mid m < x\} \, \mathrm{m} = 2^r y$

- x is an odd number, then $x = y$ and $r = 0$
- $x = 2$, then $y = 1$ and $r = 1$
- x is a prime number, then $x = y$ and $r = 0$
- x is neither a prime nor an odd, then $x = m_1 m_2$ and $m_1, m_2 < x$

$$x = 2^{r_1} y_1 2^{r_2} y_2 = 2^{r_1 + r_2} \, y_1 y_2 = 2^r y$$

is (r, y) unique?

Dirichlet drawer principle

Solution (cont'd):

$x = 2^{r_1} y_1 2^{r_2} r_2 = 2^{r_1 + r_2}\, y_1 y_2 = 2^r y$ But, is (r, y) unique?

<u>Prove by contradiction:</u> Assume there are more than one pair defines x in the given form.

$$2^{r_i} y_i = 2^{r_j} y_j$$

for $r_i > r_j \Rightarrow$ $2^{r_i} y_i = 2^{r_j} y_j \Rightarrow 2^{r_i - r_j} y_i = y_j$

$\Rightarrow y_j \neq 2p + 1\ (even)$

Dirichlet drawer principle

Solution:

Part2: Using pigeonhole principle

$f: \boldsymbol{X_m} \rightarrow \boldsymbol{Y}$ $\quad x = y\,2^r \Rightarrow y = \frac{x}{2^r}$ $\quad \boldsymbol{Y} \subseteq [\boldsymbol{2n}]$: set of odd numbers

$$|\boldsymbol{X_m}| \geq n + 1 \wedge |\boldsymbol{Y}| = n$$

$$\exists p, q \in \boldsymbol{X_m};\ f(p) = f(q) = y \in \boldsymbol{Y}$$

$$p = 2^s y,\ q = 2^t y \wedge p > q$$

$$\boxed{\Rightarrow \exists a \in N^+ \wedge s = a + t, [p = 2^{a+t} y = 2^a q]}$$

Defining a function by using Noetherian ordered set Recurrence relation

1. Creating a Noetherian ordered-set

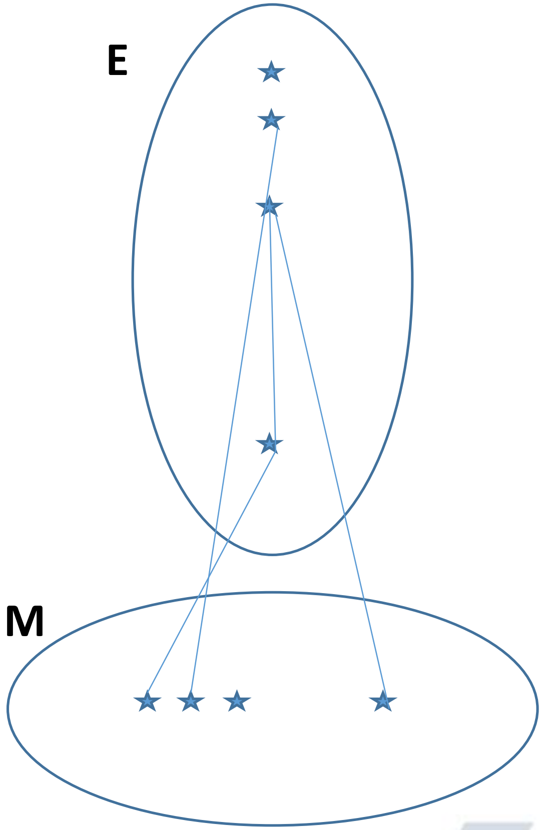
Declarations:

- $(E, \leq)$ is a well-ordered set
- $M \cap E = \emptyset$ where M is any non-empty set

$\leq$ order relation can be extended on $M \cup E$ by employing

$$\forall m, x\ (m \in M \wedge x \in E\ ) \Longrightarrow m \ll x$$

$G = M \cup E$, $(\boldsymbol{G}, \ll)$ is a Noetherian ordered-set



Additional Reads

Reads:

- Discrete Math. and its applications, K.H. Rosen
  - Chapters 6 and 9
- TBD