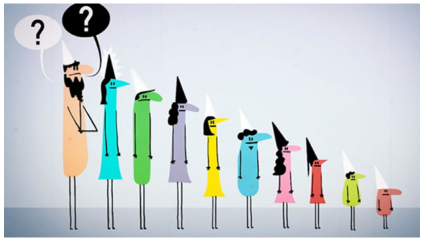
Unit 3

Relations

Albert Sung

The Prisoner Hat Riddle



- There is a line of n prisoners, $P_1, P_2, \ldots P_n$.
- Each wears a white or a black hat randomly.
- Each one can see the hats of the prisoners in front of him, but cannot see his own hat (or the hat of anyone behind him).
- Everyone has to guess and call out the color of his own hat starting from P_1, then P_2, and so on.
- Prisoners who call out incorrectly will be shot.
- **Problem:** Find a strategy that would guarantee that *at most one prisoner* is shot.

The Prisoner Hat Riddle

- https://www.youtube.com/watch?v=N5vJSNXPEwA&t=3s (4.5 min)

Outline of Unit 3

- 3.1 Definition of Relations
- 3.2 Properties of Relations
- 3.3 Equivalence Relations
- 3.4 Partial Orders

Unit 3.1

Definition of Relations

What is a Relation?

- A binary relation R from a set A to a set B is a subset of the Cartesian product $A \times B$.
- In particular, a binary relation R on a set A is a subset of A^2.
  - (This is the special case when $A = B$.)

- Given $(x, y) \in A \times B$, x is related to y,

$$\boxed{x \; R \; y \leftrightarrow (x, y) \in R.}$$

Two different ways to represent a relation.

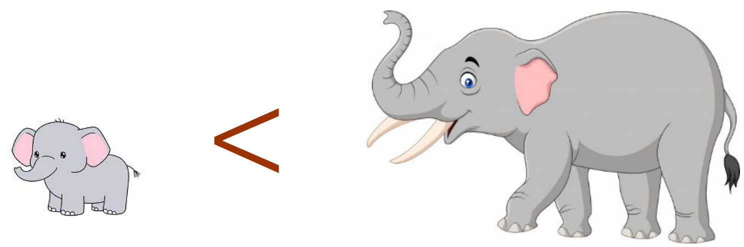
  - Relation is the fundamental notion underlying relational databases and their query languages.

Examples

Marriage in HK

- Let M and F be the sets of all men and all women in HK, respectively.
- $R_{\text{marriage}} \subseteq M \times F$
- $(x, y) \in R_{\text{marriage}}$ iff x is a husband of y.

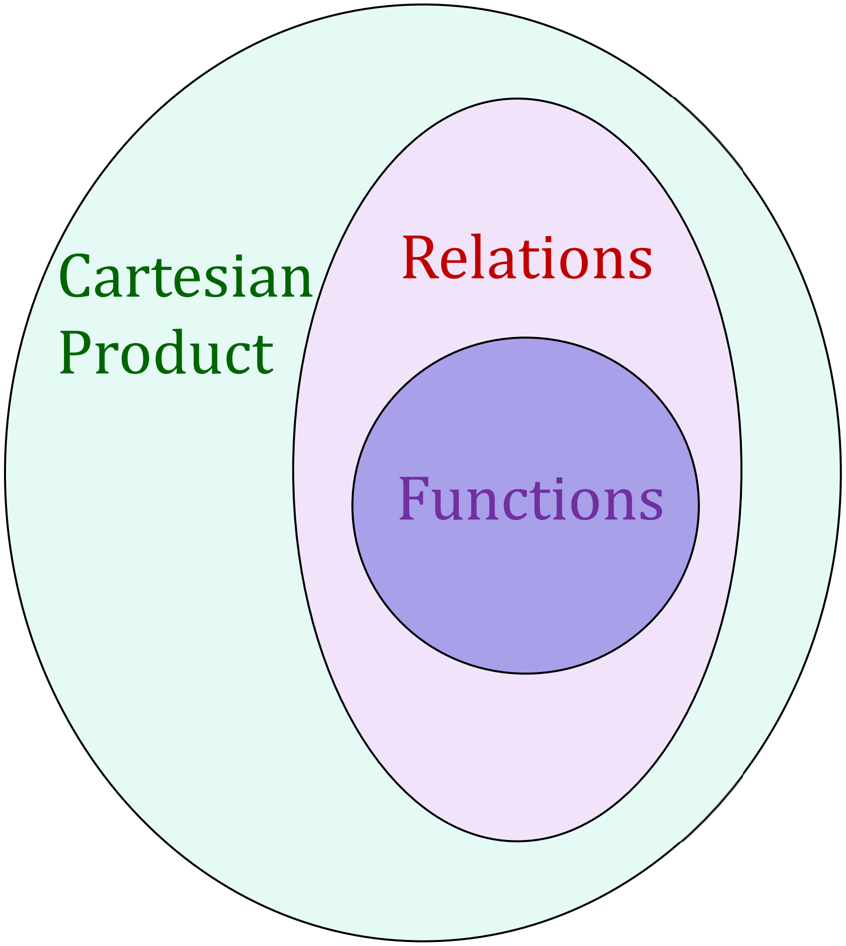
Less-Than on $\mathbb{R}$



- $R_{\text{less}} \subseteq \mathbb{R}^2$
- $(x, y) \in R_{\text{less}}$ iff $x < y$.

Functions and Relations

- Functions are a special class of relations:
  - $f(x) = y$ means xRy.
  - For each x, there exists one and only one y such that xRy.
- All functions are relations but not all relations are functions.



Inverse of a Relation

- Let R be a relation from A to B.
- The inverse relation R^{-1} from B to A is defined as follows:

$$\boxed{R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}}$$

Just flip over the ordered pair.

- Classwork:

  What is the inverse relation of

  i. the marriage relation?

  ii. the less-than relation?

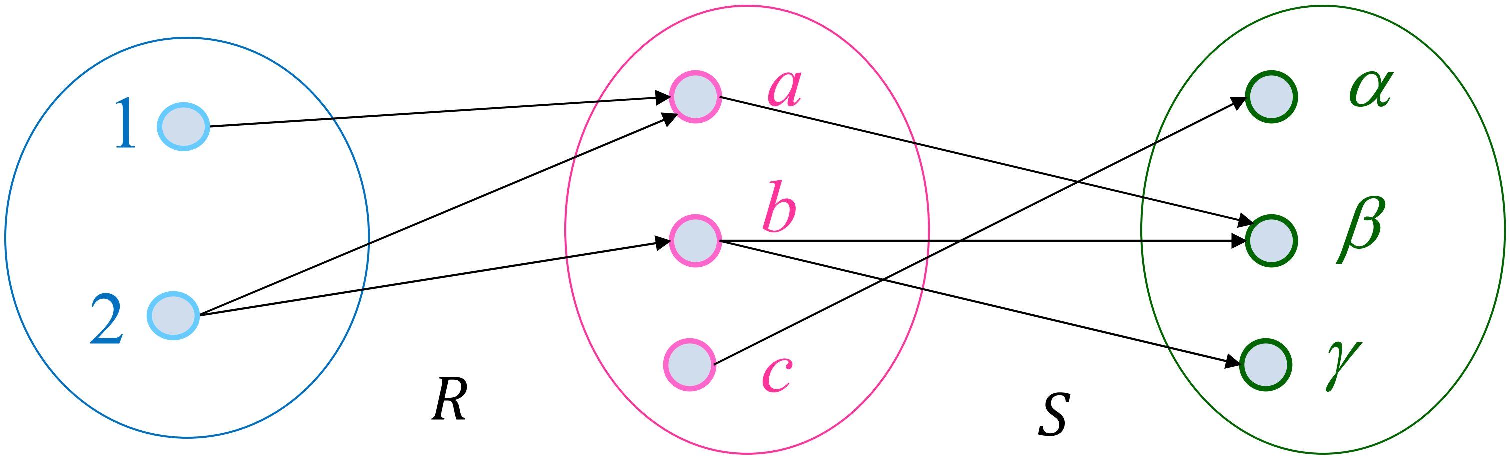
Composition of Relations

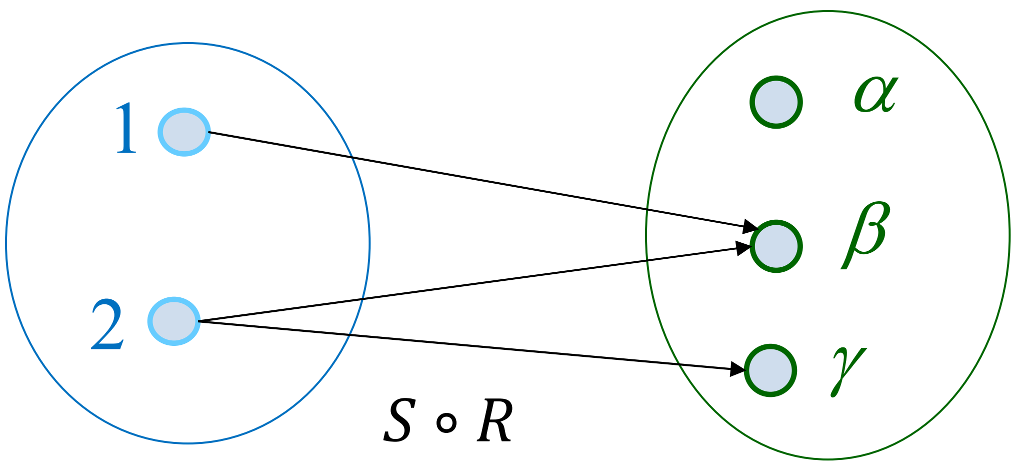
- Given $R \subseteq A \times B$ and $S \subseteq B \times C$, the composition of R with S, written $S \circ R$, is defined by

$$a\ (S \circ R)\ c \text{ iff } \exists b \in B,\ aRb\ \wedge\ bSc.$$

- $S \circ R$ may be read as "S circle R".

Illustration





Classwork

Let xFy be the relation "x is the father of y".
Let xSy be the relation "x is a sister of y".

a) What is $x(F \circ F)y$?
b) What is $x(F \circ S)y$?

k-ary Relations

- In general, a k-ary relation R is a subset of the Cartesian product $A_1 \times A_2 \times \cdots \times A_k$.
- $k = 2$: binary relation
  - Focus of this unit (except the next section).
- $k = 3$: ternary relation
  - Example of a ternary relation:
    - (HKID, Name, Date of Birth) on HK Population
- $k = 1$: unary relation
  - The same as subset.

Three Examples

1) The set of prime numbers is a unary relation on Z_+.
2) The set of twin prime pairs is a binary relation on Z_+^2.
   - (a, b) is a twin prime pair if both a and b are primes and $b - a = 2$.
     - e.g. $(3, 5), (5, 7), (11{,}13)$ are twin prime pairs.
3) The set $\{(a, b, c) \in Z_+^3 : c^2 = a^2 + b^2\}$ is a ternary relation on Z_+^3.
   - An element of this set is called a Pythagorean triple.

Unit 3.2

Properties of Relations

Reflexivity

- A relation R on a set A is reflexive if every element of A is related to itself:

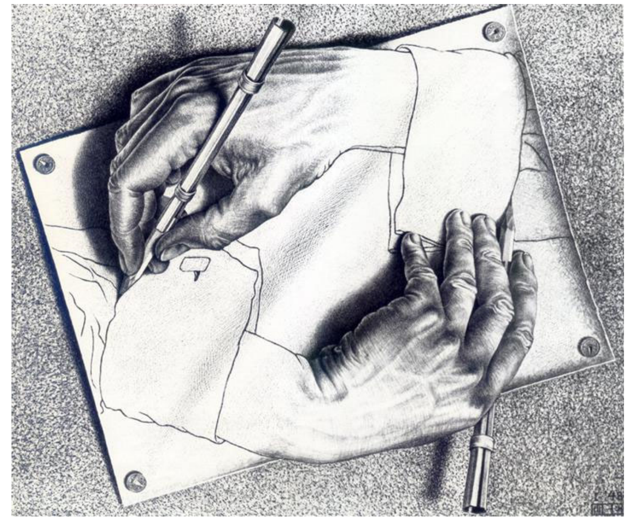
$$\boxed{\forall x \in A, xRx}$$

- Example: Equal on $\mathbb{R}$
  - The equal relation is reflexive because $\forall x \in \mathbb{R}, x = x$.

Symmetry

- A relation R on a set A is symmetric if

$$\forall x, y \in A, xRy \longrightarrow yRx$$



- Example: Same Parity
  - Define a relation P on $\mathbb{Z}$ as

    $$m\ P\ n \ \leftrightarrow m - n \text{ is even}$$

  - P is symmetric because

    $$mPn \longrightarrow nPm.$$

m and *n* are of the same parity if they are both odd or both even.

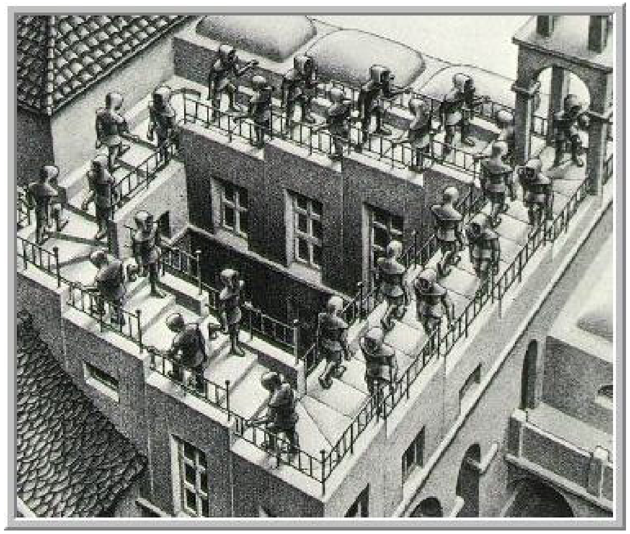
Transitivity

- A relation R on a set A is transitive if

$$\forall x, y, z \in A, (xRy \land yRz) \longrightarrow xRz$$

- Example: Less than on $\mathbb{R}$
  - The less-than relation is transitive because

    $x < y$ and $y < z$ implies $x < z$.



How come?

Antisymmetry

- A relation R on a set A is antisymmetric if

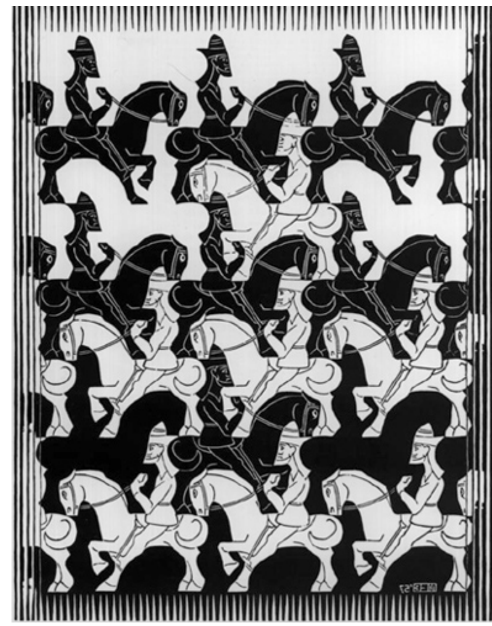
$$\forall x, y \in A, (xRy \wedge yRx) \longrightarrow x = y$$

- Example: Less than or equal to
  - Define a relation P on Z as

    $$m\ P\ n \ \leftrightarrow m \leq n$$

  - P is antisymmetric because

    if $m \leq n$ and $n \leq m$, then $m = n$.



Classwork

- Consider the subset relation $\subseteq$ on sets.

a) Is it reflexive?

b) Is it symmetric?

c) Is it transitive?

d) Is it antisymmetric?

Unit 3.3

Equivalence Relations

Equivalence Relation

- A relation R on a set A is an equivalence relation if R is reflexive, symmetric, and transitive.

- Example: Parallel Lines
  - Let A be the set of all straight lines in elementary geometry.
  - $l_1 \; R_{\text{parallel}} \; l_2 \leftrightarrow l_1 \parallel l_2$
  - It can be verified that R_{parallel} is an equivalence relation.

Classwork

- Let R be the relation on Z^2 defined by

$$(a, b)\ R\ (m, n) \ \text{ iff } \ ab = mn.$$

- Is R an equivalence relation?

Example: Congruence Modulo n

- **Definition**: Two numbers a and b are congruent modulo n if they have the same remainder when divided by n. We write

$$a \equiv b \pmod{n}.$$

Is it an equivalence relation?

- Note the following:
  - $a \equiv b \pmod{n}$ iff $a - b$ is divisible by n.
  - $a \equiv a + kn \pmod{n}$ for all integer k.
  - In particular, if r is the remainder when a is divided by n, then $a \equiv r \pmod{n}$.

Check the three conditions…

1) Reflexive
   - $a \equiv a \pmod{n}$.
2) Symmetric
   - If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
3) Transitive
   - If $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

- Equivalence relation characterizes the similarity between objects; two objects are "equal" in some sense.
  - In this example, related objects have the same remainder when divided by n.

Equivalence Class

- Let R be an equivalence relation on A.
- For each $a \in A$, the equivalence class of a is defined as

$$[a] = \{x \in A \mid xRa\}.$$

Why not aRx?

  - Note: it is a subset of A.
- Example: Congruence Modulo 3 on $\mathbb{Z}$
  - $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$
  - $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$
  - $[2] = ?$
  - $[3] = ?$

Example: Fractions

- Let $F \triangleq \left\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\right\}$.
- Define R on F by $\frac{a}{b} R \frac{c}{d}$ iff $ad = bc$.
- It is easy to check that R is an equivalence relation.
- The equivalence classes include, for example,

$$\left[\frac{1}{1}\right] = \left\{\frac{1}{1}, \frac{2}{2}, \frac{3}{3}, \dots\right\}, \left[\frac{1}{2}\right] = \left\{\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots\right\}, \left[\frac{2}{3}\right] = \left\{\frac{2}{3}, \frac{4}{6}, \frac{6}{9}, \dots\right\}.$$

- They are called rational numbers.
- The set of all the equivalence classes (i.e., rational numbers) is denoted by $\mathbb{Q}$.

Property 1: Nothing is Left Out

- Property 1: Given an equivalence relation on A, every element of A belongs to some equivalent class, i.e.,

$$\forall x \in A, \exists y \in A, x \in [y]$$

- Proof:
  - Due to reflexivity, $\forall x \in A, x \in [x]$.

Q.E.D.

Property 2: No Partial Overlapping

- Property 2: Given an equivalence relation,

$$\forall x, y \in A, \underbrace{[x] \cap [y] = \Phi}_{\text{disjoint}} \text{ or } \underbrace{[x] = [y]}_{\text{equal}}.$$

How to show two sets are equal?

- Proof: $(p \vee q \equiv {\sim}p \longrightarrow q)$
  - Suppose $[x] \cap [y] \neq \Phi$. We want to show $[x] = [y]$.
  - Let c belongs to both $[x]$ and $[y]$.
    - i.e., cRx and cRy (c exists because $[x]$ and $[y]$ are assumed non-disjoint.)
  - Take any element a from $[x]$. Then aRc.
  - By transitivity, aRc and $cRy \Rightarrow aRy$
  - By definition, $aRy \Rightarrow a \in [y]$.
  - Therefore, $[x] \subseteq [y]$.
  - Similarly, we can show that $[y] \subseteq [x]$. *Q.E.D.*

Partition of the set A

- Combining the two properties, the collection of all equivalence classes form a partition of A.
  - Note: A can be an infinite set.

- Example: mod 7 on $\{1, 2, \dots, 31\}$.
  - $[4] = \{4, 11, 18, 25\}$ (Sun)
  - $[5] = \{5, 12, 19, 26\}$ (Mon)

    $\vdots$
  - $[3] = \{3, 10, 17, 24, 31\}$ (Sat)

Seven equivalence classes

Classwork

Consider the relation R on the set of integers, where xRy iff $x - y$ is a multiple of 2.

a) Is R an equivalence relation?
   i. reflexive?
   ii. symmetric?
   iii. transitive?

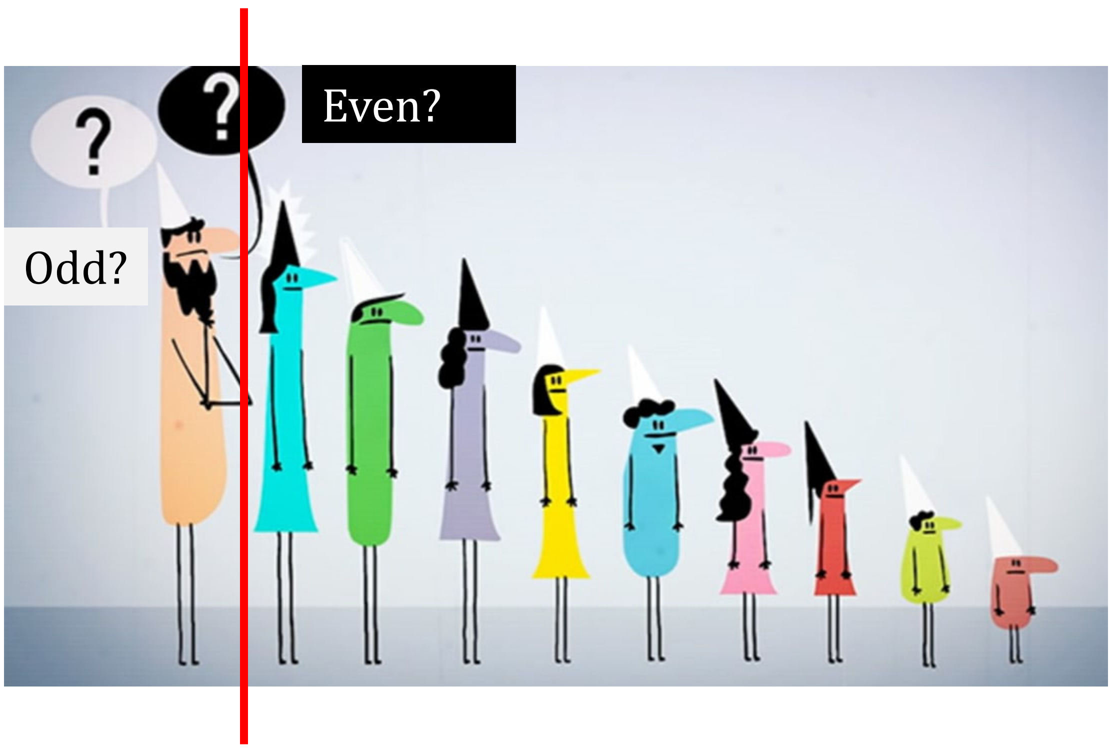
b) If so, what are the equivalence classes?

Example: Parity Relation

- Let $\{0, 1\}^n$ be the set of all binary sequences of length n.
- Let R_{parity} be the relation on $\{0, 1\}^n$ such that $xR_{\text{parity}}y$ iff the numbers of 1's in x and and in y are both odd or both even.
- For example, let $n = 3$. Then, $(111, 010) \in R_{\text{parity}}$, since both binary sequences have an odd number of ones.
- It is easy to verify that R_{parity} is an equivalence relation.

Example: Parity Relation

- Two equivalence classes:
  - [00000…000] (all zero)
  - [00000…001] (only the last bit is 1)



Strategy: The last person declares which equivalence class he sees.

Unit 3.4

Partial Orders

Partial Orders

- A relation R on a set A is a partial order if R is reflexive, antisymmetric, and transitive.

- Example:
  - Let R be the "divides" relation on $\mathbb{Z}_+$.
  - In other words, $aRb \leftrightarrow a|b$ (which means a divides b).
  - Reflexive: a always divides itself.
  - Antisymmetric: if $a|b$ and $b|a$, then $a = b$.
  - Transitive: if $a|b$ and $b|c$, then $a|c$.

Example: Less Than or Equal to

- It is easy to show that "less than or equal to" (over $\boldsymbol{Z}$, $\boldsymbol{Q}$ or $\boldsymbol{R}$) is a partial order.
  - Reflexive: $a \leq a$
  - Antisymmetric: $(a \leq b) \land (b \leq a) \longrightarrow (a = b)$
  - Transitive: $(a \leq b) \land (b \leq c) \longrightarrow (a \leq c)$

- A partial order R is often denoted by $\leq$.
  - i.e., aRb is denoted by $a \leq b$.

Classwork: Prefix of a String

- Consider the English alphabet, Σ = {a, b, c, …, z}.
- A string over Σ is a sequence of letters in Σ.
  - e.g. “information” is a string.
- A string x is a prefix of a string y if $y = xv$, for some string v.
  - e.g. “info” is a prefix of “information”
- Is “prefix” a partial order?
  - Reflexive?
  - Antisymmetric?
  - Transitive?

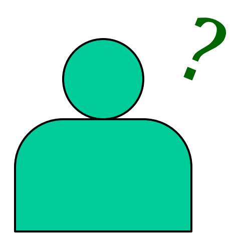
Greatest and Maximal Elements

- An element a is called the greatest element if $x \leq a$ for all $x \in A$.
  - Here $x \leq a$ means xRa.

It is larger than any others.

- An element a is called a maximal element if there is no $x \in A$ such that $a \leq x$ and $a \neq x$.

No one is larger than it.

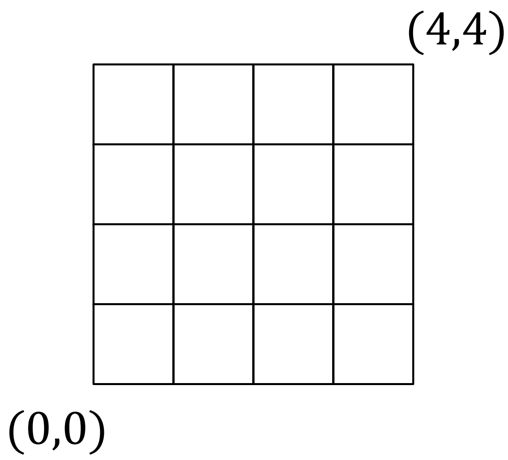


Least elements and minimal elements can be defined similarly.

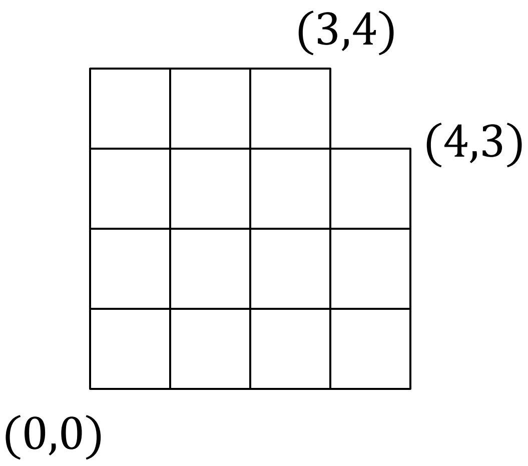
Classwork: Integer Grid

- Consider the partial order $(x_1, y_1) \leq (x_2, y_2)$ iff $x_1 \leq x_2$ and $y_1 \leq y_2$.
- What are the greatest element and maximal element in each of the following cases?

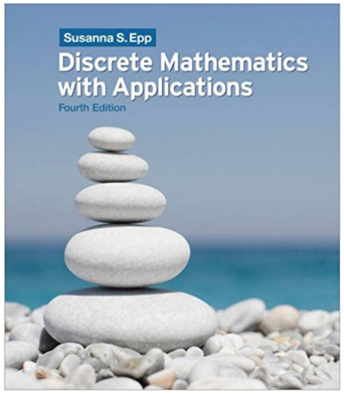
a)



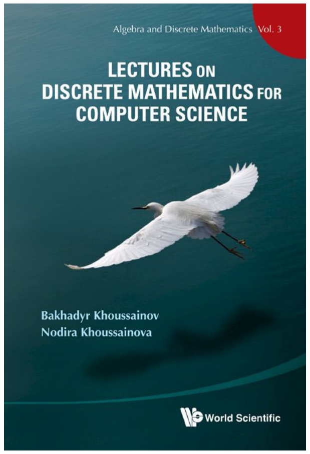
b)



Recommended Reading



- Chapter 8, S. S. Epp, *Discrete Mathematics with Applications*, 4th ed., Brooks Cole, 2010.



- Chapters 11-13, B. Khoussainov and N. Khoussainova, *Lectures on Discrete Mathematics for Computer Science*, World Scientific, 2012.