CSE 20
DISCRETE MATH

SPRING 2016

http://cseweb.ucsd.edu/classes/sp16/cse20-ac/

Today's learning goals

- Define and compute the cardinality of a set: Finite sets, countable sets, uncountable sets
- Use functions to compare the sizes of sets
- Determine and prove whether a given binary relation is
  - symmetric
  - antisymmetric
  - reflexive
  - transitive
- Represent equivalence relations as partitions and vice versa
- Define and use the congruence modulo m equivalence relation

Cardinality

Rosen Defn 3 p. 171

- Finite sets — $|A| = n$ for some nonnegative int n
- Countably infinite sets — $|A| = |\mathbf{Z}^+|$ (informally, can be listed out)
- Uncountable sets — Infinite but not in bijection with $\mathbf{Z}^+$

Cardinality

Rosen p. 172

- Countable sets A is finite or $|A| = |\mathbb{Z}^+|$ (informally, can be listed out)

Examples: $\emptyset$ $\{x \in \mathbb{Z} | x^2 = 1\}$ $\mathcal{P}(\{1,2,3\})$ $\mathbb{Z}^+$

and also …

- the set of **odd positive** integers Example 1
- the set of **all integers** Example 3
- the set of **positive rationals** Example 4
- the set of **negative rationals**
- the set of **all rationals**
- the set of **binary strings**

$|Z^+| \neq |R|$

Rosen example 5, page 173-174

Cantor's diagonalization argument

Theorem: For every set A, $|A| \neq |\mathcal{P}(A)|$

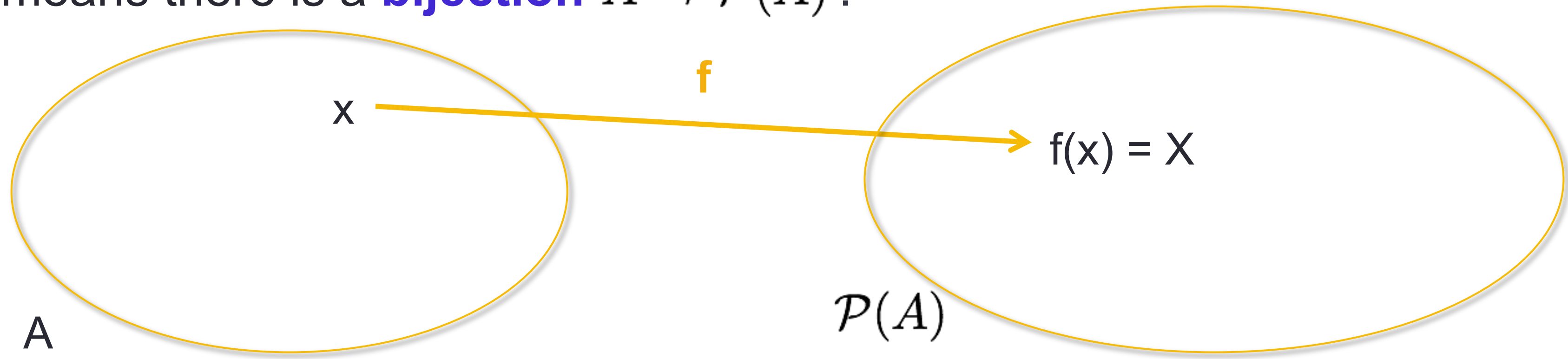
$|Z^+| \neq |R|$

Cantor's diagonalization argument

Theorem: For every set A, $|A| \neq |\mathcal{P}(A)|$

Proof: (Proof by contradiction)

Assume towards a contradiction that $|A| = |\mathcal{P}(A)|$. By definition, that means there is a **bijection** $A \to \mathcal{P}(A)$.

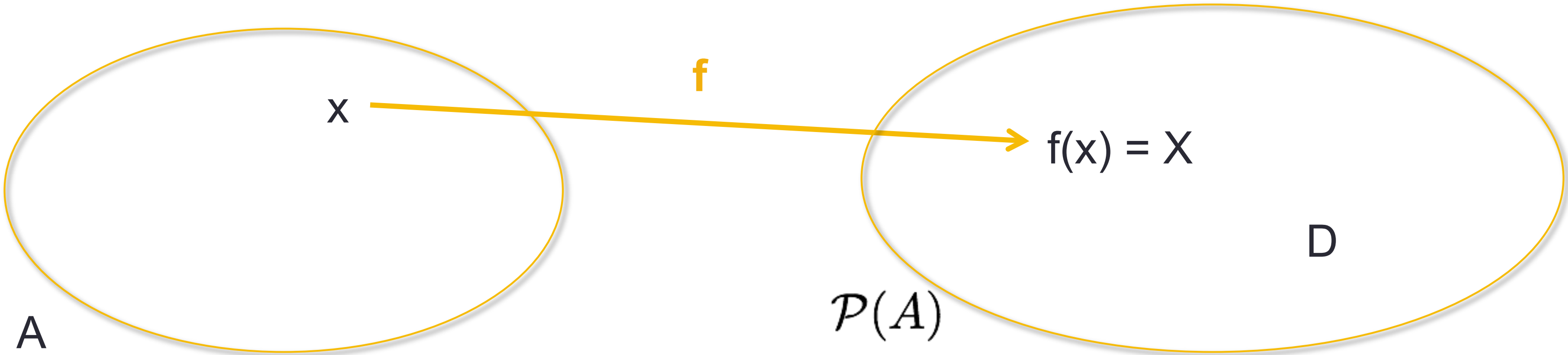


$|Z^+| \neq |R|$

Cantor's diagonalization argument

Consider the subset D of A defined by, for each a in A:

$$a \in D \qquad \text{iff} \qquad a \notin f(a)$$



$|Z^+| \neq |R|$

Cantor's diagonalization argument

Consider the subset D of A defined by, for each a in A:

$$a \in D \qquad \text{iff} \qquad a \notin f(a)$$

Define d to be the pre-image of D in A under f f(d) = D

Is d in D?

- If yes, then by definition of D, $d \notin f(d) = D$ **a contradiction!**
- Else, by definition of D, $\neg(d \notin f(d))$ so $d \in f(D) = D$ **a contradiction!**

Cardinality

Rosen p. 172

- Uncountable sets

Infinite but not in bijection with $\mathbf{Z}^+$

Examples: the power set of any countably infinite set

and also …

- the set of **real** numbers — Example 5
- (0,1) — Example 6 (++)
- (0,1] — Example 6 (++)

Exercises 33, 34

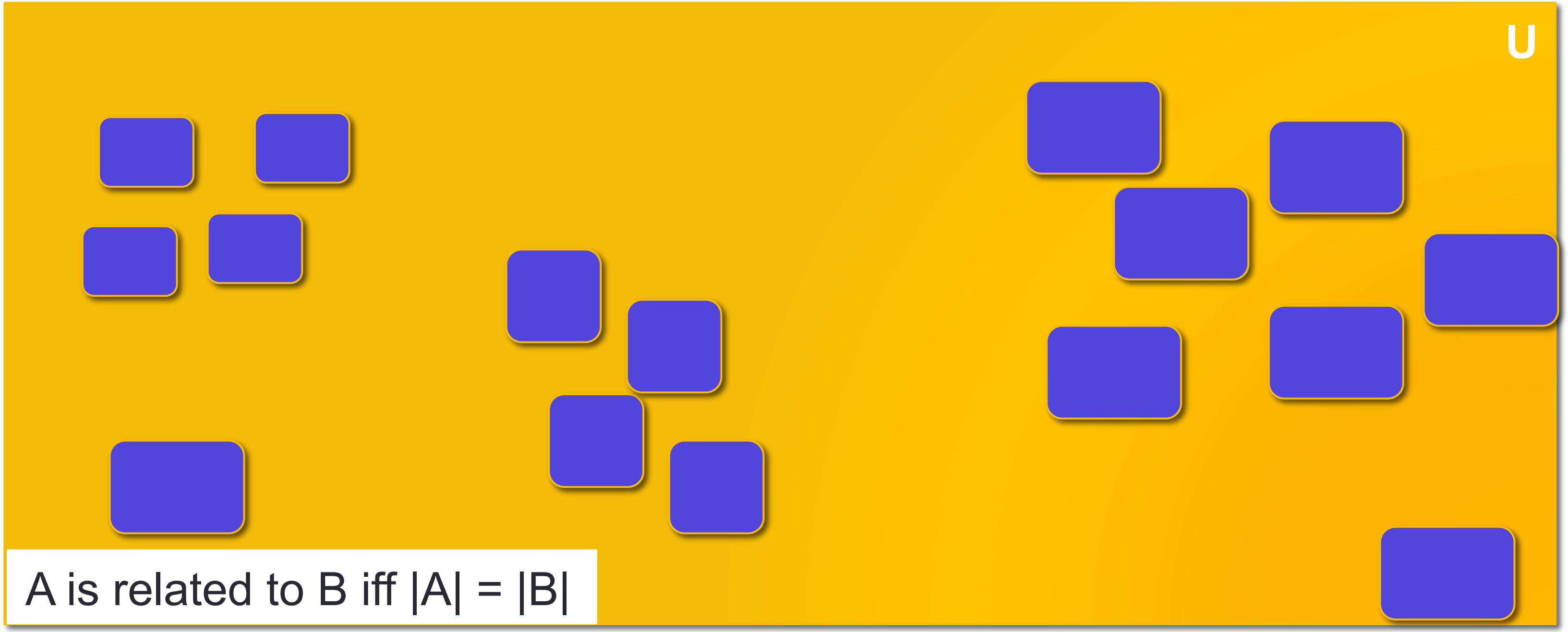
Cardinality and subsets

Suppose A and B are sets and $A \subseteq B$.

A. If A is finite then B is finite.
B. If A is countable then B is uncountable.
C. If B is infinite then A is finite.
D. If B is uncountable then A is uncountable.
E. None of the above.

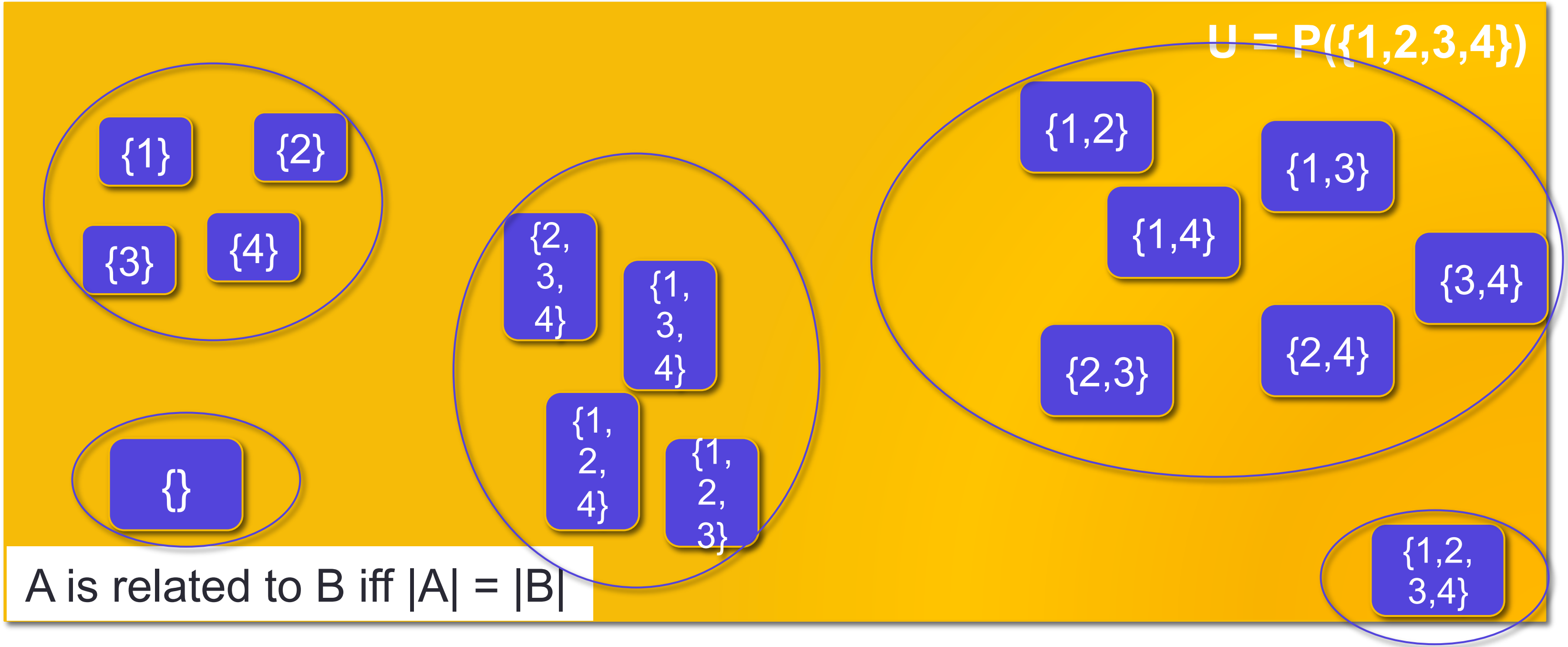
Size as a relation

- Cardinality lets us compare and group sets.



Size as a relation

- Cardinality lets us compare and group sets.



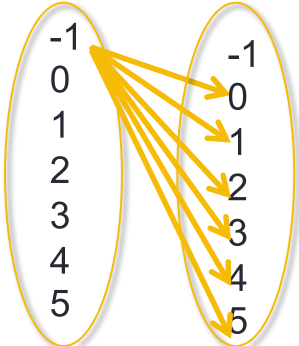
Relations, more generally *Rosen Sections 9.1, 9.3 (second half), 9.5, 9.6*

- Let A, B be sets. **Binary relation from A to B** is (any) subset of A x B.

Examples

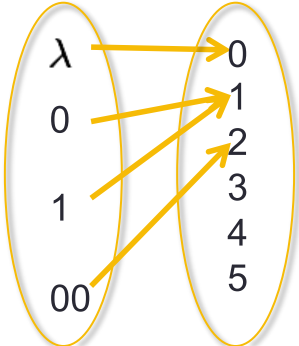
A = B = **Z**

R={(x,y) : x < y}



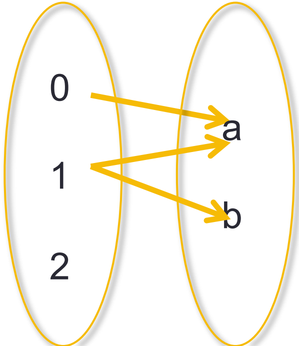
A = {0,1}* B=**N**

R={(w, n) : |w|=n}



A = {0,1,2} B={a,b}

R={(0,a), (1,a), (1,b)}



Relation on a set A

Rosen pp 576-578

R is subset of A x A. It is called

reflexive iff $\forall a(\ (a,a) \in R\ )$

symmetric iff $\forall a \forall b(\ (a,b) \in R \to (b,a) \in R\ )$

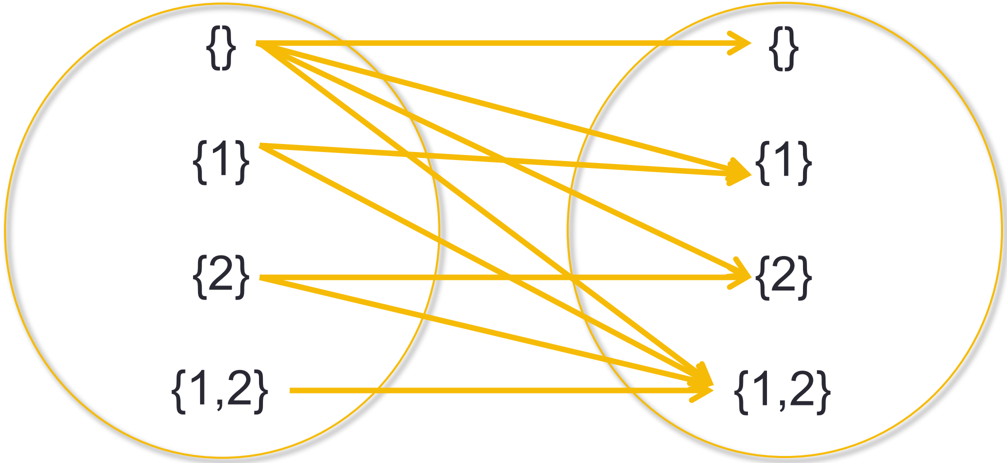
antisymmetric iff $\forall a \forall b(\ [(a,b) \in R \wedge (b,a) \in R] \to a = b\ )$

transitive iff $\forall a \forall b \forall c(\ [(a,b) \in R \wedge (b,c) \in R] \to (a,c) \in R\ )$

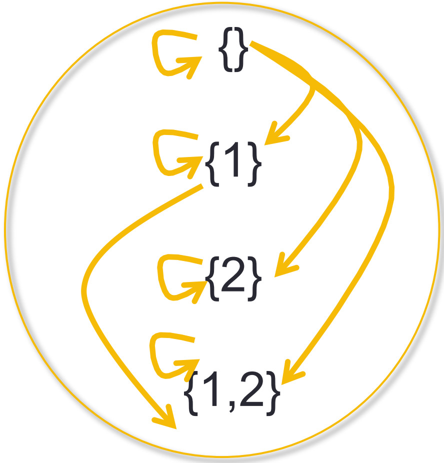
New representation of relations on a set A

$A = \mathcal{P}(\{1,2\})$ $\quad$ $X \; R \; Y$ iff $X \subseteq Y$

Old



New



Relation on a set A

Rosen pp 576-578

R is subset of A x A. It is called

reflexive iff $\forall a(\ (a, a) \in R\ )$ **self loops**

symmetric iff $\forall a \forall b(\ (a, b) \in R \rightarrow (b, a) \in R\ )$ **paired arrows**

antisymmetric iff $\forall a \forall b(\ [(a, b) \in R \wedge (b, a) \in R] \rightarrow a = b\ )$

transitive iff $\forall a \forall b \forall c(\ [(a, b) \in R \wedge (b, c) \in R] \rightarrow (a, c) \in R\ )$ **chains collapse**

Relation on a set A, more generally

Example $A = \mathcal{P}(\{1,2\})$ $X \; R \; Y \text{ iff } X \subseteq Y$

Which of the following properties hold for R?

A. Reflexive, i.e. $\forall a(\ (a,a) \in R\ )$

B. Symmetric, i.e. $\forall a \forall b(\ (a,b) \in R \rightarrow (b,a) \in R\ )$

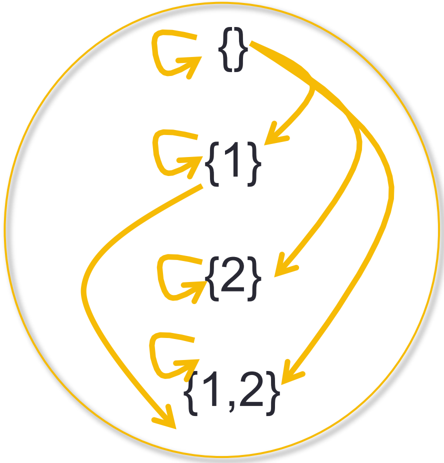
C. Antisymmetric, i.e.

$$\forall a \forall b(\ [(a,b) \in R \wedge (b,a) \in R] \rightarrow a = b\ )$$

D. Transitive, i.e.

$$\forall a \forall b \forall c(\ [(a,b) \in R \wedge (b,c) \in R] \rightarrow (a,c) \in R\ )$$

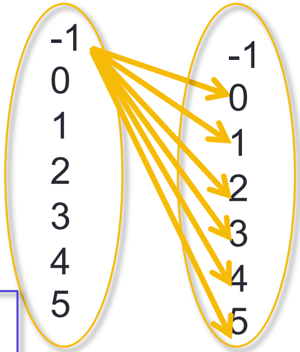
E. None of the above.



Relation on a set A, more generally

Rosen Chapter 9

Example **Z** R={(x,y) : x < y}



Which of the following properties hold for R?

A. Reflexive, i.e. $\forall a(\ (a,a) \in R\ )$
B. Symmetric, i.e. $\forall a \forall b(\ (a,b) \in R \rightarrow (b,a) \in R\ )$
C. Antisymmetric, i.e. $\forall a \forall b(\ [(a,b) \in R \wedge (b,a) \in R] \rightarrow a = b\ )$
D. Transitive, i.e. $\forall a \forall b \forall c(\ [(a,b) \in R \wedge (b,c) \in R] \rightarrow (a,c) \in R\ )$
E. None of the above.

Equivalence relations

Rosen p. 608

- Group together "similar" objects

Equivalence relations

Rosen p. 608

Two formulations

A relation R on set S is an **equivalence relation** if it is **reflexive**, **symmetric**, and **transitive**.

x R y iff x and y are "similar"

Partition S into **equivalence classes**, each of which consists of "similar" elements: collection of **disjoint**, **nonempty** subsets that have S as their **union**

x,y both in A_i iff x and y are "similar"

Equivalence relations on strings

Which of the following binary relations on $\mathcal{P}(\{1,2\})$ are equivalence relations?

A. A R_1 B iff $A \subseteq B$
B. A R_2 B iff |A| = |B|
C. A R_3 B iff A and B are disjoint
D. More than one of the above
E. None of the above

How to prove?

Equivalence relations on strings

Which of the following binary relations on {0,1}* are equivalence relations?

A. u R_1 v iff |u| = |v|
B. u R_2 v iff the first bit of u is not equal to the first bit of v
C. u R_3 v iff u is the reverse of v
D. More than one of the above
E. None of the above

How to prove?

The example

Rosen p. 240

For a,b in **Z** and m in **Z⁺** we say **a is congruent to b mod m** iff

m | (a-b)

i.e.

$$\exists q(a - b = qm)$$

and in this case, we write

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

Which of the following is true?

A. $5 \equiv 10 \pmod{3}$
B. $5 \equiv 1 \pmod{3}$
C. $5 \equiv 3 \pmod{3}$
D. $5 \equiv -1 \pmod{3}$
E. None of the above.

The example

Rosen p. 240

Claim: Congruence mod m is an equivalence relation

Proof:

Reflexive?
Symmetric?
Transitive?

What partition of the integers is associated with this equivalence relation?

Next up

- Modular arithmetic