CSE 20
DISCRETE MATH

Winter 2017

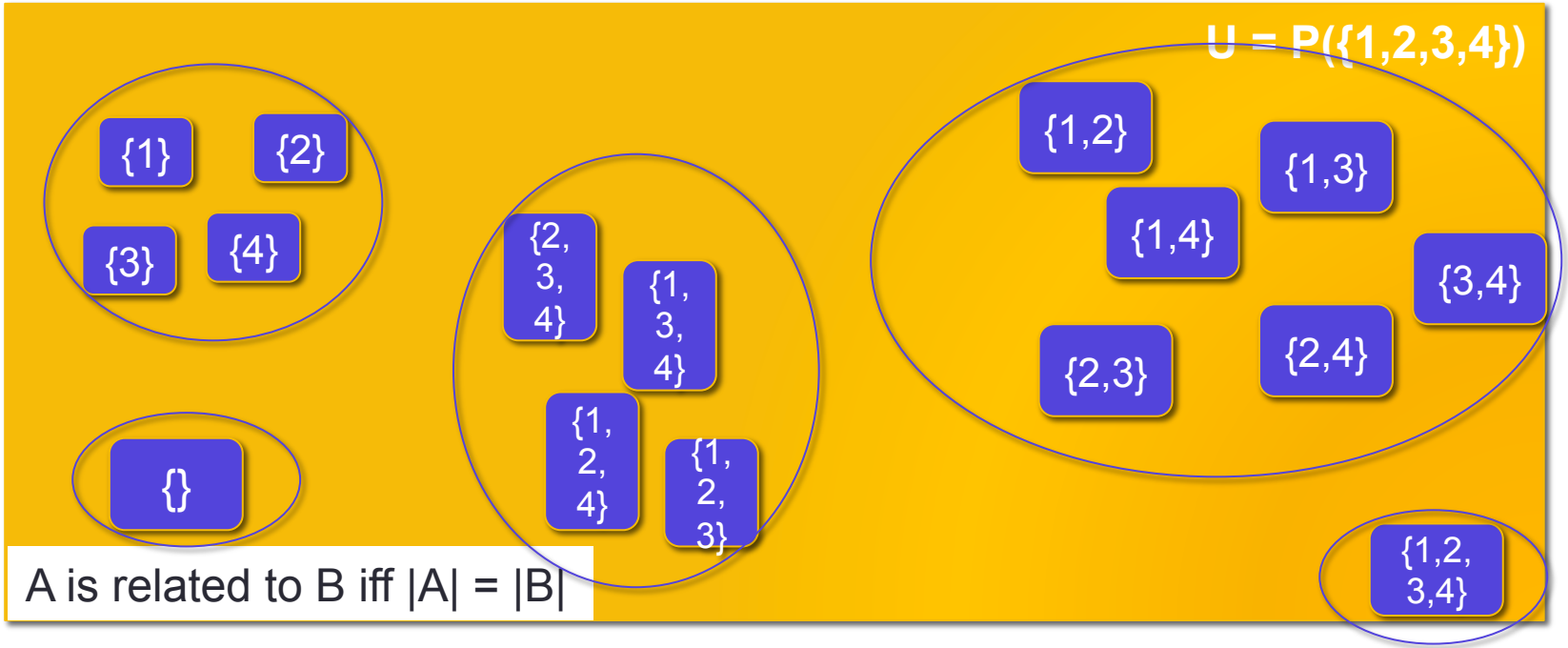
http://cseweb.ucsd.edu/classes/wi17/cse20-ab/

Today's learning goals

- Determine whether a relation is an equivalence relation by determining whether it is
  - Reflexive
  - Symmetric
  - Transitive
- Represent equivalence relations as partitions and vice versa
- Define and use the congruence modulo m equivalence relation

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**	$R_1 = \{(x,y) \mid x < y\}$	$1\ R_1\ 2$ but not $(2\ R_1\ 1)$
A = B= {0,1}*	$R_2 = \{(w, u) \mid l(w) = l(u)\}$	$10\ R_2\ 00$ but not $(0\ R_2\ 10)$
A = B= {0,1,2}	$R_3 = \{(0,0), (0,2), (2,0)\}$	$0\ R_3\ 2$ but not $(0\ R_3\ 1)$

Relation on a set A

Rosen pp 576-578

A relation R is called

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

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

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

Relation on a set A

Rosen pp 576-578

A relation R is called

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

R_1 = {(x,y) | x < y} on A = **Z**
R_2 = {(w, u) | l(w) = l(u)} on A = {0,1}*
R_3 = {(0,0), (0,2), (2,0)} on A = {0,1,2}

Which of these relations is reflexive?
A. All of them B. Just R_1
C. R_2 and R_3 D. Some other combination

Relation on a set A

Rosen pp 576-578

A relation R is called

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

R_1 = {(x,y) | x < y} on A = **Z**
R_2 = {(w, u) | l(w) = l(u)} on A = {0,1}*
R_3 = {(0,0), (0,2), (2,0)} on A = {0,1,2}

Which of these relations is symmetric?
A. All of them B. Just R_1
C. R_2 and R_3 D. Some other combination

Relation on a set A

Rosen pp 576-578

A relation R is called

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

R_1 = {(x,y) | x < y} on A = **Z**
R_2 = {(w, u) | l(w) = l(u)} on A = {0,1}*
R_3 = {(0,0), (0,2), (2,0)} on A = {0,1,2}

Which of these relations is transitive?
A. All of them B. Just R_1
C. R_2 and R_3 D. Some other combination

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 classes

Rosen p. 612

Given an equivalence relation R on set S, for a in S, the **equivalence of clas**

$$[a]_R = \{s \mid (a,s) \text{ is in } R\}$$

Theorem 1: Let R be an equivalence relation on a set A. For elements a,b of A

i. a R b iff
ii. [a] = [b] iff
iii. [a]∩ [b] is nonempty.

Relation to classes

Rosen p. 608

Given a relation R on set S, its **equivalence classes** are the sets

$$[a]_R = \{s \mid (a,s) \text{ is in } R\}$$

Example $R=\{(w, u) \mid l(w) = l(u)\}$ on $S = \{0,1\}^*$

$[0]_R = \{0,1\} = [1]_R$

$[00]_R = \{00,01,10,11\} = [01]_{R=} = [10]_{R=} = [11]_R$

etc.

Partition to relation

Rosen p. 608

The set of integers can be partitioned into four sets

{0, 4, 8, 12, …, -4, -8, -12, …}

{1, 5, 9, 13, …, -3, -7, -11, …}

{2, 6, 10, 14, …, -2, -6, -10, …}

{3, 7, 11, 15, …, -1, -5, -9, …}

What equivalence relation on **Z** has these sets as its equivalence classes?

A. xRy iff x **mod** y = 4
B. xRy iff x **mod** 4 = y **mod** 4
C. xRy iff x **div** 4 = y
D. xRy iff x **div** 4 = y **div** 4
E. None of the above

The example

Rosen p. 240

For a,b in **Z** and m in $\mathbf{Z}^+$ we say **a is congruent to b mod m** iff

$$m \mid (a-b)$$

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?

The example

Rosen p. 240

Claim: Congruence mod m is an equivalence relation

Congruence classes: $[a]_m$ **= {s | (a,s) is in R} = {s | a mod m = s mod m}**

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

E.g. m=6 $[0]_6 = \{ s : 0 \equiv s \pmod 6 \}$

{0, 6, 12, 18, 24, …}
{1, 7, 13, 19, 25, …}
{2, 8, 14, 20, 26, …}
{3, 9, 15, 21, 27, …}
{4, 10, 16, 22, 28, …}
{5, 11, 17, 23, 29, …}

Arithmetic modulo *m*

Rosen p. 242-243

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Modular addition and multiplication are well-defined on equivalence classes!

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Application 1: Last digit

What's the last digit of 2017^{2017}?
A. 1
B. 3
C. 9
D. 7
E. Can't tell without a calculator.

Last digit of decimal representation of n is n **mod** 10

Modular operations

We saw that, for all integers a,b and all positive integers m,

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m) (b \bmod m)) \bmod m$$

Which of the following is also true?

A. $(a-b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$
B. $(a/b) \bmod m = ((a \bmod m) / (b \bmod m)) \bmod m$
C. $a^b \bmod m = ((a \bmod m)^{(b \bmod m)}) \bmod m$
D. More than one of the above.
E. None of the above.

Modular operations

$(a-b) \bmod m = ((a \bmod m) - (b \bmod m)) \bmod m$

$(-b) \bmod m = (m-b) \bmod m$

$(a/b) \bmod m = ((a \bmod m) / (b \bmod m)) \bmod m$

Counterexample: a = 16, b = 8, m = 10

$a^b \bmod m = ((a \bmod m)^{(b \bmod m)}) \bmod m$

Counterexample: a = 2, b= 10, m = 10

Application 2: Proof by cases

Claim: The square of each integer is either divisible by 4 or has remainder 1 upon division by 4.

Proof:

Induction?

Contradiction?

Exhaustive?

Application 2: Proof by cases

Claim: The square of each integer is either divisible by 4 or has remainder 1 upon division by 4.

Proof: Let n be an integer and consider its remainder upon division by r.

Four cases: remainder is 0, 1, 2, or 3.

…

Application 3: Pseudorandom generators

Rosen p. 288

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

Parameters:

- modulus m
- multiplier a (2 <= a < m)
- increment c (0 <= c < m)
- seed x_0 (0 <= x_0 < m)

What's the maximum number of terms before the sequence starts to repeat?

A. m
B. a
C. c
D. x_0
E. Depends on the parameters; maybe never!

Application 3: Pseudorandom generators

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

Parameters:

- modulus m
- multiplier a (2 <= a < m)
- increment c (0 <= c < m)
- seed x_0 (0 <= x_0 < m)

m=8, a=5, c=1, x_0=1 1, 6, 7, 4, 5, 2, 3, 0, 1, 6, 7, 4, 5, 2, 3, …

m=8, a=5, c=4, x_0=1 1, 1, 1, 1, 1, …