Today's learning goals

- 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
- Define and use the posets given by: ≤, |, subset inclusion, prefix, lexicographic
- Define and prove properties of maximal and minimal elements
Let A, B be sets. **Binary relation from A to B** is (any) subset of $A \times B$.

**Examples**

- $A = B = \mathbb{Z}$
  - $R = \{(x, y) : x < y\}$

- $A = \{0,1\}^*$ $B = \mathbb{N}$
  - $R = \{(w, n) : |w| = n\}$

- $A = \{0,1,2\}$ $B = \{a,b\}$
  - $R = \{(0,a), (1,a), (1,b)\}$

Rosen Sections 9.1, 9.3 (second half), 9.5, 9.6
Relation on a set $A$

$R$ is subset of $A \times A$. It is called

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

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

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

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

*Rosen pp 576-578*
New representation of relations on a set $A$

$$A = \mathcal{P}(\{1, 2\})$$

$X \ R \ Y$ iff $X \subseteq Y$

![Diagram showing the old and new representations of relations on a set $A$. The old representation has arrows pointing from each subset to itself, while the new representation includes additional arrows connecting subsets to themselves.]
Relation on a set $A$

$R$ is subset of $A \times A$. 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 \( \forall a \forall b \ ([(a, b) \in R \land (b, a) \in R] \rightarrow a = b) \)

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

*Rosen pp 576-578*
Relation on a set $A$, more generally

$A = \mathcal{P}(\{1, 2\})$

$X \ R \ Y \ \text{iff} \ X \subseteq Y$

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.

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

D. Transitive, i.e.

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

E. None of the above.
Relation on a set \( A \), more generally

*Example* \( \mathbb{Z} \)

\[ R = \{(x,y) : x < y\} \]

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. \( \forall a \forall b ( (a, b) \in R \land (b, a) \in R \rightarrow a = b ) \)
D. Transitive, i.e. \( \forall a \forall b \forall c ( (a, b) \in R \land (b, c) \in R \rightarrow (a, c) \in R ) \)
E. None of the above.
Partial order relations

- A relation $R$ on set $S$ is a **partial ordering** iff it is **reflexive**, **antisymmetric**, and **transitive**.

*Examples on the set of integers:* "less than or equal", "greater than or equal"
*Example on the set of positive integers:* divisibility
*Example on power set of a set:* subset inclusion
*Example on set of binary strings:* "is a prefix of"
Orders on set of strings

For $u,v$ in $\{0,1\}^*$

$u$ is a **prefix** of $v$ iff $\exists w (v = uw)$

Which of the following is true?

A. $\forall x\forall y (x$ is a prefix of $y)$
B. $\exists x\forall y (x$ is a prefix of $y)$
C. $\exists x\forall y (y$ is a prefix of $x)$
D. $\forall x\forall y (y$ is a prefix of $x \lor y$ is a prefix of $x)$
E. None of the above.
Lexicographic order

• Is there a way to **totally order** the set of binary strings?
Lexicographic order

Is there a way to totally order the set of binary strings?

Here's one way …

\[ u < v \quad \text{iff} \quad \begin{align*}
& u \text{ is a prefix of } v, \\
& \text{or, the letter in } u \text{ in the first position where } u \text{ and } v \text{ differ is 0.}
\end{align*} \]
Maximal and minimal elements

For $R$ an order relation on $S$ and for any subset $T$ of $S$:

- $q$ in $T$ is **minimum** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow qRx) \)

- $q$ in $T$ is **minimal** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow \neg(xRq)) \)

- $q$ in $T$ is **maximum** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow xRq) \)

- $q$ in $T$ is **maximal** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow \neg(qRx)) \)
Maximal and minimal elements

For $R$ an order relation on $S$ and for any subset $T$ of $S$:

- $q$ in $T$ is **minimum** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow qRx) \)
- $q$ in $T$ is **minimal** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow \neg(xRq)) \)
- $q$ in $T$ is **maximum** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow xRq) \)
- $q$ in $T$ is **maximal** element of $T$ \( \forall x((x \in T \land x \neq q) \rightarrow \neg(qRx)) \)

Does the poset of \{0,1\}#$^*$ with prefix partial order have a minimal element? a maximal element? a minimum element? a maximum element?

What if we remove the empty string from the set?
Equivalence relations

• Group together "similar" objects

Rosen p. 608
Equivalence relations

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 \{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?
For $a,b$ in $\mathbb{Z}$ and $m$ in $\mathbb{Z}^+$ 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.
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