HW7 due Saturday
LM8 released tomorrow
Review session during exam week TBD

Fall 2017

http://cseweb.ucsd.edu/classes/fa17/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
Cardinality recap

Finite

- \{0,1\}
- \{a\}
- \{1\}
- \{a,b\}
- \{Empty set\}
- Empty set

Countably infinite

- \{0,1\}^*
- \mathbb{N}
- \mathbb{Z}
- \mathbb{Q}
- \mathbb{Z}^+ \times \mathbb{Z}^+

Uncountable

- \mathbb{R}
- P(P(\emptyset))
- \emptyset
- P(\mathbb{N})
- (0,1)
### Binary relations

#### Rosen Ch 9 p. 573

**Student Last Name** | **Major**
---|---
Ackermann | Math-CS
Guo | Cog Sci
Kumar | CS
Yau | Economics
Yau | CS

---

<table>
<thead>
<tr>
<th>$\mathcal{P}({a,b})$</th>
<th>$\mathcal{P}({a,b})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>empty set</td>
<td>empty set</td>
</tr>
<tr>
<td>${a}$</td>
<td>${a}$</td>
</tr>
<tr>
<td>${a}$</td>
<td>${b}$</td>
</tr>
<tr>
<td>${b}$</td>
<td>${a}$</td>
</tr>
<tr>
<td>${b}$</td>
<td>${b}$</td>
</tr>
<tr>
<td>${a,b}$</td>
<td>${a,b}$</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>(1, 2, 4, 8)</th>
<th>(1, 2, 4, 8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

---

Write as graph:

- **A**
- **B**
Let $A$ be a set.

**Binary relation on $A$** is (any) subset of $A \times A$.

**How to visualize / represent?**

Directed graph

$$|X| = |Y| ?$$

$$\emptyset \subseteq \{a, b\}$$

$$(\emptyset, \emptyset)$$

$$(\{a\}, \{b\})$$

$$(\{ab\}, \{a^3\})$$

Fill in rest
Relations, more generally

Let $A$ be a set.

**Binary relation on $A$** is (any) subset of $A \times A$.

**Examples**

Let $A = \mathbb{Z}$

$R_1 = \{(x,y) \mid x < y\}$

$1 \ R_1 2 \quad \text{aka} \ (1, 2) \in R$

$\text{not}(2 \ R_1 1) \quad \text{aka} \ (2, 1) \notin R$
Relations, more generally

Let $A$ be a set.

**Binary relation on $A$** is (any) subset of $A \times A$.

*Examples*

$A = \{0,1\}^*$

$R_2 = \{(w, u) \mid l(w) = l(u)\}$

$10 \not\in R_2,$ $00$

not($0 \, R_2 \, 10$)
Relations, more generally

Let $A$ be a set.

**Binary relation on $A$** is (any) subset of $A \times A$.

**Examples**

$A = \{0, 1, 2\}$

$R_3 = \{(0, 0), (0, 2), (2, 0)\}$

$0 R_3 2$

not $(0 R_3 1)$

\[ \text{Function } \{ (x, f(x)) \mid x \in \text{domain} \} \]
Equivalence relations

Group together "similar" objects

Rosen p. 608
Equivalence relations

Partition $S$ into \textbf{equivalence classes}, each of which consists of "similar" elements: collection of \textbf{disjoint, nonempty} subsets that have $S$ as their \textbf{union}

$x,y$ both in $A_i$ iff $x$ and $y$ are "similar"
Relation on a set $A$

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 $\forall a \forall b \forall c \ [ (a, b) \in R \land (b, c) \in R ] \rightarrow (a, c) \in R$
A relation $R$ is called reflexive iff $\forall a( (a, a) \in R )$

- $R_1 = \{(x, y) \mid x < y\}$ on $A = \mathbb{Z}$
- $R_2 = \{(w, u) \mid l(w) = l(u)\}$ 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
A relation $R$ is called **symmetric** iff
\[ \forall a \forall b \ (a, b) \in R \rightarrow (b, a) \in R \]

- $R_1 = \{(x,y) \mid x < y\}$ on $A = \mathbb{Z}$
- $R_2 = \{(w, u) \mid l(w) = l(u)\}$ 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

---

**Check**
- $a = 0, b = 0$
- $a = 0, b = 2$
- $a = 2, b = 0$
Relation on a set A

A relation $R$ is called transitive iff

$$\forall a \forall b \forall c \left( (a, b) \in R \land (b, c) \in R \implies (a, c) \in R \right)$$

if $a = b$ need

$$\left( (a, a) \in R \land (a, c) \in R \right) \implies (a, c) \in R$$

$R_1 = \{(x, y) \mid x < y\}$ on $A = \mathbb{Z}$

$R_2 = \{(w, u) \mid l(w) = l(u)\}$ 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

Two formulations

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

\[ x \, R \, y \iff x \text{ and } y \text{ are "similar"} \]

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

\[ x, y \text{ both in } A_i \iff x \text{ and } y \text{ are "similar"} \]
Equivalence classes

Given an equivalence relation $R$ on set $S$, for $a$ in $S$, the equivalence of class of $a$ is

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

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

i. $a R b$  \(\iff\)\n
ii. $[a] = [b]$  \(\iff\)\n
iii. $[a] \cap [b]$ is nonempty.
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.
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 \(\mathbb{Z}\) 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

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?
*The* example

Claim: Congruence mod m is an equivalence relation

Congruence classes: \([a]_m = \{s \mid (a,s) \text{ is in } R\} = \{s \mid 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, \ldots\} \quad \{3, 9, 15, 21, 27, \ldots\}

\{1, 7, 13, 19, 25, \ldots\} \quad \{4, 10, 16, 22, 28, \ldots\}

\{2, 8, 14, 20, 26, \ldots\} \quad \{5, 11, 17, 23, 29, \ldots\}
Arithmetic modulo $m$

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

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

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

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
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 \(m\),

\[(a+b) \mod m = ( (a \mod m) + (b \mod m) ) \mod m\]

\[ab \mod m = ((a \mod m) (b \mod m)) \mod m\]

Which of the following is also true?

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

\[(a-b) \mod m = ( (a \mod m) - (b \mod m) ) \mod m\]

\[(-b) \mod m = (m-b) \mod m\]

\[(a/b) \mod m = ( (a \mod m) / (b \mod m) ) \mod m\]

Counterexample: \(a = 16, b = 8, m = 10\)

\[a^b \mod m = ( (a \mod m)^{(b \mod m)} ) \mod m\]

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?
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

\[ x_{n+1} = (ax_n + c) \mod m \]

Parameters:
- modulus \( m \)
- multiplier \( a \) \((2 \leq a < m)\)
- increment \( c \) \((0 \leq c < m)\)
- seed \( x_0 \) \((0 \leq x_0 < m)\)

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

\[ x_{n+1} = (ax_n+c) \mod m \]

Parameters:
- modulus \( m \)
- multiplier \( a \) \( (2 \leq a < m) \)
- increment \( c \) \( (0 \leq c < m) \)
- seed \( x_0 \) \( (0 \leq x_0 < m) \)

\( m=8, \ a=5, \ c=1, \ x_0=1 \)
\[ 1, 6, 7, 4, 5, 2, 3, 0, 1, 6, 7, 4, 5, 2, 3, \ldots \]

\( m=8, \ a=5, \ c=4, \ x_0=1 \)
\[ 1, 1, 1, 1, 1, \ldots \]