Discrete Mathematics
(Relations)

Pramod Ganapathi
Department of Computer Science
State University of New York at Stony Brook

January 24, 2021
Are these functions?

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
</table>
| • Are these functions?  
  – rational \( p = \text{rational } q \)  
  – \( m < n \)  
  – \( d \) does not divide \( n \)  
  – \( n \) leaves a remainder of 5 when divided by \( d \)  
  – line \( \ell_1 \) is parallel to line \( \ell_2 \)  
  – person \( a \) is a parent of person \( b \)  
  – triangle \( t_1 \) is congruent to triangle \( t_2 \)  
  – edge \( e_1 \) is adjacent to edge \( e_2 \)  
  – matrix \( A \) is orthogonal to matrix \( B \)  
  No! (Because an input is mapped to more than one output.)  
| • **What are these mappings called?**  
  Relations! |
Functions vs. Relations

- Functions
  - \( n^2 \)
  - \( n - 2 \)
  - \( 2^n \)
  - \( \log x \)
  - \( x^{1/x} \)
  - \( \sin x \)

- Relations
  - Congruence modulo
  - Congruent
  - Parallel
  - Orthogonal
  - Adjacent

- Symbols
  - \(<, >, \leq, \geq\)
Functions vs. relations

\[ y = x^2 \]

\[ x = y^2 \]

<table>
<thead>
<tr>
<th></th>
<th>( y = x^2 )</th>
<th>( y = \pm \sqrt{x} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function?</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Relation?</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Functions vs. relations

<table>
<thead>
<tr>
<th></th>
<th>$y = x$</th>
<th>$y \geq x$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function?</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Relation?</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### Definition

- If $A$ and $B$ are sets, then a **binary relation** from $A$ to $B$ is a subset of $A \times B$.
- We say that $x$ is related to $y$ by $R$, written $x \mathrel{R} y$, if, and only if, $(x, y) \in R$. Denoted as $x \mathrel{R} y \iff (x, y) \in R$.

### Relationship

- **Set of all functions** is a proper subset of the set of all relations.
Example: Marriage relation

![Marriage relation diagram with Male and Female sets, and connections between M1, M2, M3, M4 to F1, F2, F3, F4, F5.]
Example: Less than

Problem

- A relation $L : \mathbb{R} \rightarrow \mathbb{R}$ as follows.
  
  For all real numbers $x$ and $y$, $(x, y) \in L \iff x \, L \, y \iff x < y$.

  Draw the graph of $L$ as a subset of the Cartesian plane $\mathbb{R} \times \mathbb{R}$.

Solution

- $L = \{(-10.678, 30.23), (17.13, 45.98), (100/9, 200), \ldots\}$

- Graph:
**Problem**

- Define a relation $C : \mathbb{Z} \rightarrow \mathbb{Z}$ as follows.
  For all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, $m C n \iff m - n$ is even.
- Prove that if $n$ is any odd integer, then $n C 1$.

**Solution**

- $A = \{(2, 4), (56, 10), (-88, -64), \ldots\}$
  $B = \{(7, 7), (57, 11), (-87, -63), \ldots\}$
  $C = A \cup B$

- Proof. $(n, 1) \in C \iff n C 1 \iff n - 1$ is even
  Suppose $n$ is odd i.e., $n = 2k + 1$ for some integer $k$. This implies that $n - 1 = 2k$ is even.
Example: Congruence modulo 2
Inverse of a relation

- Male: $M_1, M_2, M_3, M_4$
- Female: $F_1, F_2, F_3, F_4, F_5$

The diagram illustrates the relationship between males and females, showing the inverse of a relation.
**Inverse of a relation**

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Let $R$ be a relation from $A$ to $B$. Then <strong>inverse relation</strong> $R^{-1}$ from $B$ to $A$ is: $R^{-1} = {(y, x) \in B \times A \mid (x, y) \in R}$.</td>
</tr>
<tr>
<td>• For all $x \in A$ and $y \in B$, $(x, y) \in R \iff (y, x) \in R^{-1}$.</td>
</tr>
</tbody>
</table>
Example: Inverse of a finite relation

Problem

• Let $A = \{2, 3, 4\}$ and $B = \{2, 6, 8\}$.
  Let $R : A$ to $B$. For all $(a, b) \in A \times B$, $a \ R \ b \iff a \mid b$

• Determine $R$ and $R^{-1}$. Draw arrow diagrams for both.
  Describe $R^{-1}$ in words.

Solution

• $R = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$
  $R^{-1} = \{(2, 2), (6, 2), (8, 2), (6, 3), (8, 4)\}$

• For all $(b, a) \in B \times A$,
  $(b, a) \in R^{-1} \iff b$ is a multiple of $a$
Example: Inverse of an infinite relation

Problem

• Define a relation $R$ from $\mathbb{R}$ to $\mathbb{R}$ as follows:
  For all $(u, v) \in \mathbb{R} \times \mathbb{R}$, $u R v \iff v = 2|u|$.
• Draw the graphs of $R$ and $R^{-1}$ in the Cartesian plane.
  Is $R^{-1}$ a function?

Solution

• $R^{-1}$ is not a function. Why?
**Definition**

- A relation on a set $A$ is a relation from $A$ to $A$.
- The resulting arrow diagram is a directed graph possibly containing loops.
### Problem

- Let $A = \{3, 4, 5, 6, 7, 8\}$. Define relation $R$ on $A$ as follows. For all $x, y \in A$, $x R y \iff 2 \mid (x - y)$. Draw the graph of $R$.

### Solution

![Graph of relation $R$](image)
Reflexivity, symmetry, and transitivity

Properties

- Set \( A = \{2, 3, 4, 6, 7, 9\} \)
  
  Relation \( R \) on set \( A \) is: \( \forall x, y \in A, x R y \iff 3 \mid (x - y) \)

- **Reflexivity.** \( \forall x \in A, (x, x) \in R. \)
- **Symmetry.** \( \forall x, y \in A, \text{ if } (x, y) \in R, \text{ then } (y, x) \in R. \)
- **Transitivity.**
  
  \( \forall x, y, z \in A, \text{ if } (x, y) \in R \text{ and } (y, z) \in R, \text{ then } (x, z) \in R. \)
Example

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
</table>
| \( A = \{0, 1, 2, 3\} \).  
\( R = \{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (2, 2), (3, 0), (3, 3)\} \).  
Is \( R \) reflexive, symmetric, and transitive? |

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
</table>
| • Reflexive. \( \forall x \in A, (x, x) \in R \).  
• Symmetric. \( \forall x, y \in A, \text{ if } (x, y) \in R, \text{ then } (y, x) \in R \).  
• Not transitive. e.g.: \( (1, 0), (0, 3) \in R \) but \( (1, 3) \notin R \).  
\( \exists x, y, z \in A, \text{ if } (x, y) \in R \text{ and } (y, z) \in R, \text{ then } (x, z) \notin R \). |

[Diagram showing relationships between elements of set A with arrows indicating reflexive, symmetric, and non-transitive conditions.]
Example

**Problem**

- $A = \{0, 1, 2, 3\}$. $R = \{(0, 0), (0, 2), (0, 3), (2, 3)\}$.
  Is $R$ reflexive, symmetric, and transitive?

**Solution**

- **Not reflexive.** e.g.: $(1, 1) \notin R$. $\exists x \in A, (x, x) \notin R$.
- **Not symmetric.** e.g.: $(0, 3) \in R$ but $(3, 0) \notin R$.
  $\exists x, y \in A$, if $(x, y) \in R$, then $(y, x) \notin R$.
- **Transitive.**
  $\forall x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$. 
**Example**

**Problem**

- \( A = \{0, 1, 2, 3\} \). \( R = \{(0, 1), (2, 3)\} \).
  Is \( R \) reflexive, symmetric, and transitive?

**Solution**

- **Not reflexive.** e.g.: \((0, 0) \notin R\). \( \exists x \in A, (x, x) \notin R \).
- **Not symmetric.** e.g.: \((0, 1) \in R \) but \((1, 0) \notin R\).
  \( \exists x, y \in A, \) if \((x, y) \in R\), then \((y, x) \notin R\).
- **Transitive.** Why?
  \( \forall x, y, z \in A, \) if \((x, y) \in R\) and \((y, z) \in R\), then \((x, z) \in R\).
Equivalence relation and equivalence class

Definition

- Relation $R$ on set $A$ is an equivalence relation iff $R$ is reflexive, symmetric, and transitive.
- Equivalence class of element $a$, denoted by $[a]$, for an equivalence relation is defined as:
  $$[a] = \{ x \in A \mid (x, a) \in R \}.$$
Example: Less than

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Suppose $R$ is a relation on $\mathbb{R}$ such that $x R y \iff x &lt; y$. Is $R$ an equivalence relation?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not reflexive. e.g.: $0 \not&lt; 0$. $\exists x \in \mathbb{R}, x \not&lt; x$.</td>
</tr>
<tr>
<td>• Not symmetric. e.g.: $0 &lt; 1$ but $1 \not&lt; 0$. $\exists x, y \in \mathbb{R},$ if $x &lt; y$, then $y \not&lt; x$.</td>
</tr>
<tr>
<td>• Transitive. $\forall x, y, z \in \mathbb{R},$ if $x &lt; y$ and $y &lt; z$, then $x &lt; z$. So, $R$ is not an equivalence relation.</td>
</tr>
</tbody>
</table>
### Example: Equality (or Identity relation)

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
</table>
| • Suppose $R$ is a relation on $\mathbb{R}$ such that $x R y \iff x = y$.  
  Is $R$ an equivalence relation? |

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
</table>
| • Reflexive. $\forall x \in \mathbb{R}, x = x$.  
| • Symmetric. $\forall x, y \in \mathbb{R}$, if $x = y$, then $y = x$.  
| • Transitive. $\forall x, y, z \in \mathbb{R}$, if $x = y$ and $y = z$, then $x = z$.  
So, $R$ is an equivalence relation.  
Equivalence classes: $[a] = \{a\}$. |
Example: Partition

Problem

- Suppose $R$ is a partition relation on $A$ such that 
  \[ \forall x, y \in A, \ x \mathrel{R} y \iff x, y \in A_i \text{ for some subset } A_i. \]
- $A = \{0, 1, 2, 3, 4\}$. Partition of $A$ is $\{\{0, 3, 4\}, \{1\}, \{2\}\}$. Is $R$ an equivalence relation?

Solution

- $R$ is reflexive, symmetric, and transitive.
- So, $R$ is an equivalence relation.
- Equivalence classes: $[0] = \{0, 3, 4\}$, $[1] = \{1\}$, and $[2] = \{2\}$. 
Example: Partition

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Suppose $R$ is a partition relation on $A$ such that $\forall x, y \in A, x R y \iff x, y \in A_i$ for some subset $A_i$. Is $R$ an equivalence relation?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
</table>
| • Reflexive. $\forall m \in A, (m, m) \in R$.  
• Symmetric. $\forall m, n \in A$, if $(m, n) \in R$, then $(n, m) \in R$.  
• Transitive.  
  $\forall m, n, p \in A$, if $(m, n) \in R$ and $(n, p) \in R$, then $(m, p) \in R$.  
So, $R$ is an equivalence relation. |
Example: Least element

Problem

- Let $X$ denote the power set of $\{1, 2, 3\}$. Suppose $R$ is a relation on $X$ such that $\forall A, B \in X \ A\ R\ B \iff$ Least element of $A$ is same as that of $B$. Is $R$ an equivalence relation?

Solution

- $R$ is reflexive, symmetric, and transitive.
- So, $R$ is an equivalence relation.
- Equivalence classes: $[\{1\}]$, $[\{2\}]$, and $[\{3\}]$. 
Example: Congruence modulo 3

Problem

• Suppose $R$ is a relation on $\mathbb{Z}$ such that $m R n \Leftrightarrow 3 \mid (m - n)$. Is $R$ an equivalence relation?

Solution

• Reflexive. $\forall m \in A, 3 \mid (m - m)$.
• Symmetric. $\forall m, n \in A$, if $3 \mid (m - n)$, then $3 \mid (n - m)$.
• Transitive.
  $\forall m, n, p \in A$, if $3 \mid (m - n)$ and $3 \mid (n - p)$, then $3 \mid (m - p)$.
So, $R$ is an equivalence relation.
### Solution

**Equivalence classes.**

Three distinct equivalence classes are \([0]\), \([1]\), and \([2]\).

\[
[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod{3}\} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}
\]

\[
[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod{3}\} = \{1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \ldots\}
\]

\[
[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod{3}\} = \{2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \ldots\}
\]

**Intuition.**

\([0]\) = Set of integers when divided by 3 leave a remainder of 0.

\([1]\) = Set of integers when divided by 3 leave a remainder of 1.

\([2]\) = Set of integers when divided by 3 leave a remainder of 2.
Definition

Let $a$ and $b$ be integers and $n$ be a positive integer. The following statements are equivalent:

- $a$ and $b$ leave the same remainder when divided by $n$.
  \[ a \mod n = b \mod n. \]
- $n$ divides $(a - b)$.
  \[ n \mid (a - b). \]
- $a$ is congruent to $b$ modulo $n$.
  \[ a \equiv b \pmod{n}. \]
- $a = b + kn$ for some integer $k$.

Examples

- $12 \equiv 7 \pmod{5}$
- $6 \equiv -6 \pmod{4}$
- $3 \equiv 3 \pmod{7}$
### Example: Congruence modulo \( n \)

<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
</table>
| • Suppose \( R \) is a relation on \( \mathbb{Z} \) such that  
\[
a \in R b \iff a \equiv b \pmod{n}.
\]  
Is \( R \) an equivalence relation? |

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
</table>
| • **Reflexive.** \( \forall a \in \mathbb{Z}, a \equiv a \pmod{n} \).  
• **Symmetric.**  
\[\forall a, b \in \mathbb{Z}, \text{ if } a \equiv b \pmod{n}, \text{ then } b \equiv a \pmod{n}.\]  
• **Transitive.**  
\[\forall a, b, c \in \mathbb{Z}, \text{ if } a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n}, \text{ then } a \equiv c \pmod{n}.\]  
So, \( R \) is an equivalence relation.  
Equivalence classes: \([0], [1], \ldots, [n - 1]\). |
Example: Congruence modulo $n$

Solution

- **$R$ is Reflexive.** Show that $\forall a \in \mathbb{Z}, n \mid (a - a)$. We know that $a - a = 0$ and $n \mid 0$. Hence, $n \mid (a - a)$.

- **$R$ is Symmetric.** Show that $\forall a, b \in \mathbb{Z}$, if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$. We see that $a \equiv b \pmod{n}$ means $n \mid (a - b)$.

Let $(a - b) = nk$, for some integer $k$.

$\Rightarrow - (a - b) = -nk$ \hspace{1cm} (multiply both sides by -1)

$\Rightarrow (b - a) = n(-k)$ \hspace{1cm} (simplify)

$\Rightarrow n \mid (b - a)$ \hspace{1cm} $(-k$ is an integer; use defn. of divisibility)

In other words, $b \equiv a \pmod{n}$. 

Solution

• \( R \) is transitive. Show that \( \forall a, b, c \in \mathbb{Z}, \text{ if } a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \), then \( a \equiv c \pmod{n} \).

We see that \( a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \) imply that \( n \mid (a - b) \) and \( n \mid (b - c) \), respectively.

Let \( (a - b) = nk \) and \( (b - c) = n\ell \), for some integers \( k \) and \( \ell \).

Adding the two equations, we get \( (a - c) = (k + \ell)n \), where \( k + \ell \) is an integer because addition is closed on integers.

By definition of divisibility, \( n \mid (a - c) \) or \( a \equiv c \pmod{n} \).
Modular arithmetic

Let \( a, b, c, d, n \) be integers with \( n > 1 \).

Suppose \( a \equiv c \pmod{n} \) and \( b \equiv d \pmod{n} \). Then

1. \( (a + b) \equiv (c + d) \pmod{n} \)
2. \( (a - b) \equiv (c - d) \pmod{n} \)
3. \( (ab) \equiv (cd) \pmod{n} \)
4. \( (a^m) \equiv (c^m) \pmod{n} \) for all positive integers \( m \)
<table>
<thead>
<tr>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What is the units digit of $1483^{8650}$?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution</th>
</tr>
</thead>
</table>
| • Units digit of $1483^{8650}$ is the units digit of $3^{8650}$.  
• Units digit of $3^0, 3^1, 3^2, 3^3,$ and $3^4$ are 1, 3, 9, 7, and 1, respectively.  
• **Periodicity** is 4. Therefore, 
• Units digit of $3^{4k+0}$ is 1.  
  Units digit of $3^{4k+1}$ is 3.  
  Units digit of $3^{4k+2}$ is 9.  
  Units digit of $3^{4k+3}$ is 7.  
• Units digit of $3^{8650} = 3^{4 \times 2162+2}$ is 9.  
• Hence, the answer is 9. |
### Problem

- Use modular arithmetic to solve the equations.

\[ 16x + 12y = 32 \quad \text{and} \quad 40x - 9y = 7. \]

### Solution

- Apply \( \text{mod} \ 3 \) on both sides of the first equation.

\[
(16x + 12y) \equiv 32 \quad \text{mod} \ 3 \\
\implies x \equiv 2 \quad \text{mod} \ 3
\]

Similarly, apply \( \text{mod} \ 3 \) on both sides of the second equation.

\[
(40x - 9y) \equiv 7 \quad \text{mod} \ 3 \\
\implies x \equiv 1 \quad \text{mod} \ 3
\]

- These two congruences are contradictory.

Hence, the system of equations does not have a solution.
Check digits are used to reduce errors universal product codes, tracking operations for shipping operations, book identification numbers (ISBNs), vehicle numbers, ID for the healthcare industry, etc.

UPC is a 12-digit number, where the last digit is the check digit.

Suppose the first 11 digits of the UPC are \(a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}\). Then the check digit can be computed using the following formula

\[
a_{12} = (210 - k) \mod 10,
\]

where

\[
k = 3(a_1 + a_3 + \cdots + a_{11}) + (a_2 + a_4 + \cdots + a_{10})
\]
### Problem
- The first eleven digits of the UPC for a package of ink cartridges are 88442334010. What is the check digit?

### Solution
- \[ k = 3(8 + 4 + 2 + 3 + 0 + 0) + (8 + 4 + 3 + 4 + 1) = 71 \]
- Check digit = \( (210 - 71) \mod 10 = 9 \)