Discrete Mathematics

Relations and Functions

H. Turgut Uyar Ayşegül Gençata Yayımlı Emre Harmancı

2001-2011

License

Topics

Relation

Definition

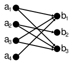
relation: $\alpha \subseteq A \times B \times C \cdots \times N$

- tuple: an element of a relation
- $\alpha \subseteq A \times B$: *binary relation*
- $\alpha \subseteq A \times A$: *binary relation on A*
- representations:
  - by drawing
  - with a matrix

Relation Example

Example

$A = \{a_1, a_2, a_3, a_4\}, B = \{b_1, b_2, b_3\}$
$\alpha = \{(a_1, b_1), (a_1, b_3), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_3), (a_4, b_1)\}$



	b_1	b_2	b_3
a_1	1	0	1
a_2	0	1	1
a_3	1	0	1
a_4	1	0	0

$$M_\alpha = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{vmatrix}$$

Composite Relation

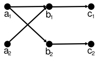
Definition

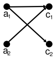
composite relation:
$\alpha \subseteq A \times B \wedge \beta \subseteq B \times C$
$\Rightarrow \alpha\beta = \{(a, c) | a \in A, c \in C, \exists b \in B[a\alpha b \wedge b\beta c)]\}$

- $M_{\alpha\beta} = M_\alpha \times M_\beta$

Composite Relation Example

Example





Composite Relation Matrix Example

Example

$$M_\alpha = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix} \qquad M_\beta = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{vmatrix} \qquad M_{\alpha\beta} = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{vmatrix}$$

Composite Relation Associativity

Theorem

$(\alpha\beta)\gamma = \alpha(\beta\gamma) = \alpha\beta\gamma$

Composite Relation Associativity

Proof.

$$
\begin{aligned}
& (a,d) \in (\alpha\beta)\gamma \\
\Leftrightarrow\ & \exists c[(a,c) \in \alpha\beta \wedge (c,d) \in \gamma] \\
\Leftrightarrow\ & \exists c[\exists b[(a,b) \in \alpha \wedge (b,c) \in \beta] \wedge (c,d) \in \gamma] \\
\Leftrightarrow\ & \exists b[(a,b) \in \alpha \wedge \exists c[(b,c) \in \beta \wedge (c,d) \in \gamma]] \\
\Leftrightarrow\ & \exists b[(a,b) \in \alpha \wedge (b,d) \in \beta\gamma] \\
\Leftrightarrow\ & (a,d) \in \alpha(\beta\gamma)
\end{aligned}
$$

□

Composite Relation Theorems

- $\alpha, \delta \subseteq A \times B \wedge \beta, \gamma \subseteq B \times C$
  - $\alpha(\beta \cup \gamma) = \alpha\beta \cup \alpha\gamma$
  - $\alpha(\beta \cap \gamma) \subseteq \alpha\beta \cap \alpha\gamma$
  - $(\alpha \cup \delta)\beta = \alpha\beta \cup \delta\beta$
  - $(\alpha \cap \delta)\beta \subseteq \alpha\beta \cap \delta\beta$
  - $(\alpha \subseteq \delta \wedge \beta \subseteq \gamma) \Rightarrow \alpha\beta \subseteq \delta\gamma$

Composite Relation Theorems

$\alpha(\beta \cup \gamma) = \alpha\beta \cup \alpha\gamma$.

$$
\begin{aligned}
& (x,y) \in \alpha(\beta \cup \gamma) \\
\Leftrightarrow\ & \exists z[(x,z) \in \alpha \wedge (z,y) \in (\beta \cup \gamma)] \\
\Leftrightarrow\ & \exists z[(x,z) \in \alpha \wedge ((z,y) \in \beta \vee (z,y) \in \gamma)] \\
\Leftrightarrow\ & \exists z[((x,z) \in \alpha \wedge (z,y) \in \beta) \\
& \quad \vee ((x,z) \in \alpha \wedge (z,y) \in \gamma)] \\
\Leftrightarrow\ & (x,y) \in \alpha\beta \vee (x,y) \in \alpha\gamma \\
\Leftrightarrow\ & (x,y) \in \alpha\beta \cup \alpha\gamma
\end{aligned}
$$

□

Converse Relation

Definition

$\alpha^{-1} : \{(y,x) | (x,y) \in \alpha\}$

- $M_{\alpha^{-1}} = M_\alpha^T$

Converse Relation Theorems

- $(\alpha^{-1})^{-1} = \alpha$
- $(\alpha \cup \beta)^{-1} = \alpha^{-1} \cup \beta^{-1}$
- $(\alpha \cap \beta)^{-1} = \alpha^{-1} \cap \beta^{-1}$
- $\overline{\alpha}^{-1} = \overline{\alpha^{-1}}$
- $(\alpha - \beta)^{-1} = \alpha^{-1} - \beta^{-1}$
- $\alpha \subset \beta \Rightarrow \alpha^{-1} \subset \beta^{-1}$

Converse Relation Theorems

$\overline{\alpha}^{-1} = \overline{\alpha^{-1}}$.

$$\begin{aligned} & (x,y) \in \overline{\alpha}^{-1} \\ \Leftrightarrow\ & (y,x) \in \overline{\alpha} \\ \Leftrightarrow\ & (y,x) \notin \alpha \\ \Leftrightarrow\ & (x,y) \notin \alpha^{-1} \\ \Leftrightarrow\ & (x,y) \in \overline{\alpha^{-1}} \end{aligned}$$

$\square$

Converse Relation Theorems

$(\alpha \cap \beta)^{-1} = \alpha^{-1} \cap \beta^{-1}$.

$$\begin{aligned} & (x,y) \in (\alpha \cap \beta)^{-1} \\ \Leftrightarrow\ & (y,x) \in (\alpha \cap \beta) \\ \Leftrightarrow\ & (y,x) \in \alpha \wedge (y,x) \in \beta \\ \Leftrightarrow\ & (x,y) \in \alpha^{-1} \wedge (x,y) \in \beta^{-1} \\ \Leftrightarrow\ & (x,y) \in \alpha^{-1} \cap \beta^{-1} \end{aligned}$$

$\square$

Converse Relation Theorems

$(\alpha - \beta)^{-1} = \alpha^{-1} - \beta^{-1}$.

$$\begin{aligned}(\alpha - \beta)^{-1} &= (\alpha \cap \overline{\beta})^{-1} \\ &= \alpha^{-1} \cap \overline{\beta}^{-1} \\ &= \alpha^{-1} \cap \overline{\beta^{-1}} \\ &= \alpha^{-1} - \beta^{-1}\end{aligned}$$

□

Converse Composite Relation

Theorem
$(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$

Proof.

$$\begin{aligned} & (c, a) \in (\alpha\beta)^{-1} \\ \Leftrightarrow\ & (a, c) \in \alpha\beta \\ \Leftrightarrow\ & \exists b[(a, b) \in \alpha \wedge (b, c) \in \beta] \\ \Leftrightarrow\ & \exists b[(c, b) \in \beta^{-1} \wedge (b, a) \in \alpha^{-1}] \\ \Leftrightarrow\ & (c, a) \in \beta^{-1}\alpha^{-1}\end{aligned}$$

□

Converse Composite Relation Matrix

- $M_{(\alpha\beta)^{-1}} = M_{\beta^{-1}} \times M_{\alpha^{-1}}$
- $M_{\alpha\beta}^T = M_\beta^T \times M_\alpha^T$

Converse Composite Relation Matrix Example

Example

$$M_\alpha = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{vmatrix} \qquad M_\beta = \begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{vmatrix}$$

$$M_{\alpha\beta^{-1}} = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{vmatrix}$$

Binary Relation Properties

- $\alpha \subseteq A \times A$
- $\alpha\alpha : \alpha^2$
  - $\alpha\alpha\ldots\alpha : \alpha^n$
- *identity relation*: $E = \{(x,x) | x \in A\}$
- properties: reflexivity, symmetry, transitivity

Reflexivity

reflexive
$\alpha \subseteq A \times A$
$\forall a\ [a\alpha a]$

- nonreflexive:
  $\exists a\ [\neg(a\alpha a)]$
- irreflexive:
  $\forall a\ [\neg(a\alpha a)]$

Reflexivity Examples

Example
$\mathcal{R}_1 \subseteq \{1,2\} \times \{1,2\}$
$\mathcal{R}_1 = \{(1,1),(2,2)\}$

- $\mathcal{R}_1$ is reflexive

Example
$\mathcal{R}_2 \subseteq \{1,2,3\} \times \{1,2,3\}$
$\mathcal{R}_2 = \{(1,1),(2,2)\}$

- $\mathcal{R}_2$ is nonreflexive

Reflexivity Examples

Example
$\mathcal{R} \subseteq \{1,2,3\} \times \{1,2,3\}$
$\mathcal{R} = \{(1,2),(2,1),(2,3)\}$

- $\mathcal{R}$ is irreflexive

Reflexivity Examples

Example

$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$

$(a, b) \in \mathcal{R} \equiv ab \geq 0$

- $\mathcal{R}$ is reflexive

Symmetry

symmetric

$\alpha \subseteq A \times A$

$\forall a, b[(a = b) \vee (a\alpha b \wedge b\alpha a) \vee (\neg(a\alpha b) \wedge \neg(b\alpha a))]$

$\forall a, b[(a = b) \vee (a\alpha b \leftrightarrow b\alpha a)]$

- asymmetric:
  $\exists a, b[(a \neq b) \wedge (a\alpha b \wedge \neg(b\alpha a)) \vee (\neg(a\alpha b) \wedge b\alpha a))]$
- antisymmetric:

$$\begin{aligned} & \forall a, b\ [(a = b) \vee \neg(a\alpha b) \vee \neg(b\alpha a)] \\ \Leftrightarrow\quad & \forall a, b\ [\neg(a\alpha b \wedge b\alpha a) \vee (a = b)] \\ \Leftrightarrow\quad & \forall a, b\ [(a\alpha b \wedge b\alpha a) \rightarrow (a = b)] \end{aligned}$$

Symmetry Examples

Example

$\mathcal{R} \subseteq \{1, 2, 3\} \times \{1, 2, 3\}$

$\mathcal{R} = \{(1, 2), (2, 1), (2, 3)\}$

- $\mathcal{R}$ is asymmetric

Symmetry Examples

Example

$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$

$(a, b) \in \mathcal{R} \equiv ab \geq 0$

- $\mathcal{R}$ is symmetric

Symmetry Examples

Example

$\mathcal{R} \subseteq \{1,2,3\} \times \{1,2,3\}$
$\mathcal{R} = \{(1,1),(2,2)\}$

- $\mathcal{R}$ is both symmetric and antisymmetric

Transitivity

transitive

$\alpha \subseteq A \times A$
$\forall a,b,c \; [(a\alpha b \wedge b\alpha c) \rightarrow (a\alpha c)]$

- nontransitive:
  $\exists a,b,c \; [(a\alpha b \wedge b\alpha c) \wedge \neg(a\alpha c)]$
- antitransitive:
  $\forall a,b,c \; [(a\alpha b \wedge b\alpha c) \rightarrow \neg(a\alpha c)]$

Transitivity Examples

Example

$\mathcal{R} \subseteq \{1,2,3\} \times \{1,2,3\}$
$\mathcal{R} = \{(1,2),(2,1),(2,3)\}$

- $\mathcal{R}$ is antitransitive

Transitivity Examples

Example

$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a,b) \in \mathcal{R} \equiv ab \geq 0$

- $\mathcal{R}$ is nontransitive

Converse Relation Properties

Theorem

The reflexivity, symmetry and transitivity properties are preserved in the converse relation.

Closure

- reflexive closure:
  $r_\alpha = \alpha \cup E$
- symmetric closure:
  $s_\alpha = \alpha \cup \alpha^{-1}$
- transitive closure:
  $t_\alpha = \bigcup_{i=1\ldots n} \alpha^i = \alpha \cup \alpha^2 \cup \alpha^3 \cup \cdots \cup \alpha^n$

Special Relations

predecessor - successor

$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a, b) \in \mathcal{R} \equiv a - b = 1$

- irreflexive
- antisymmetric
- antitransitive

Special Relations

adjacency

$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a, b) \in \mathcal{R} \equiv |a - b| = 1$

- irreflexive
- symmetric
- antitransitive

Special Relations

strict order
$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a, b) \in \mathcal{R} \equiv a < b$

- irreflexive
- antisymmetric
- transitive

Special Relations

partial order
$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a, b) \in \mathcal{R} \equiv a \leq b$

- reflexive
- antisymmetric
- transitive

Special Relations

preorder
$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a, b) \in \mathcal{R} \equiv |a| \leq |b|$

- reflexive
- asymmetric
- transitive

Special Relations

limited difference
$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a, b) \in \mathcal{R} \equiv |a - b| \leq m$

- reflexive
- symmetric
- nontransitive

Special Relations

comparability

$\mathcal{R} \subseteq \mathbb{U} \times \mathbb{U}$

$(a, b) \in \mathcal{R} \equiv (a \subseteq b) \vee (b \subseteq a)$

- reflexive
- symmetric
- nontransitive

Special Relations

brotherhood

- irreflexive
- symmetric
- transitive

- can a relation be symmetric, transitive and irreflexive?

Compatible Relations

Definition

compatible relation: γ

- reflexive
- symmetric

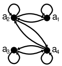
- undirected graph
- matrix representation as a triangle matrix

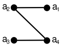
- $\alpha\alpha^{-1}$ is a compatible relation

Compatible Relation Example

Example

$$
\begin{aligned}
A &= \{a_1, a_2, a_3, a_4\} \\
\mathcal{R} &= \{ \\
&\quad (a_1, a_1), (a_2, a_2), \\
&\quad (a_3, a_3), (a_4, a_4), \\
&\quad (a_1, a_2), (a_2, a_1), \\
&\quad (a_2, a_4), (a_4, a_2), \\
&\quad (a_3, a_4), (a_4, a_3) \\
&\quad \}
\end{aligned}
$$





$$
\begin{vmatrix}
1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1
\end{vmatrix}
$$

$$
\begin{vmatrix}
1 & & \\
0 & 0 & \\
0 & 1 & 1
\end{vmatrix}
$$

Compatible Relation Example

Example ($\alpha\alpha^{-1}$)

A: persons, B: languages

$A = \{a_1, a_2, a_3, a_4, a_5, a_6\}$
$B = \{b_1, b_2, b_3, b_4, b_5\}$
$\alpha \subseteq A \times B$

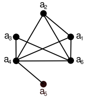
$$M_\alpha = \begin{vmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{vmatrix} \qquad M_{\alpha^{-1}} = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{vmatrix}$$

Compatible Relation Example

Example ($\alpha\alpha^{-1}$)

$\alpha\alpha^{-1} \subseteq A \times A$

$$M_{\alpha\alpha^{-1}} = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{vmatrix}$$



Compatible Class

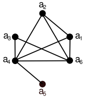
Definition

compatibility block: $C \subseteq A$
$\forall a, b\ [a \in C \wedge b \in C \rightarrow a\gamma b]$

- *maximal compatibility block*:
  not a subset of another compatibility block
- an element can be a member of more than one MCB
- complete cover: C_γ
  set of all MCBs

Compatible Block Examples

Example ($\alpha\alpha^{-1}$)



- $C_1 = \{a_4, a_6\}$
- $C_2 = \{a_2, a_4, a_6\}$
- $C_3 = \{a_1, a_2, a_4, a_6\}$ (MCC)

$$C_\gamma(A) = \{ \{a_1, a_2, a_4, a_6\}, \{a_3, a_4, a_6\}, \{a_4, a_5\} \}$$

Equivalence Relations

Definition
equivalence relation: ϵ

- reflexive
- symmetric
- transitive

- equivalence classes
- every element is a member of exactly one equivalence class

- complete cover: C_ϵ

Partitioning

- every equivalence relation *partitions* a set into equivalence classes
- every *partitioning* corresponds to an equivalence relation

Equivalence Relation Example

Example
$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$(a, b) \in \mathcal{R} \equiv 5 \mid |a - b|$

- x *mod* 5 partitions $\mathbb{Z}$ into 5 equivalence classes

References

Required Text: Grimaldi

- Chapter 5: Relations and Functions
  - 5.1. Cartesian Products and Relations
- Chapter 7: Relations: The Second Time Around
  - 7.1. Relations Revisited: Properties of Relations
  - 7.4. Equivalence Relations and Partitions

Supplementary Text: O'Donnell, Hall, Page

- Chapter 10: Relations

Function

Definition

function: $f : X \to Y$

$\forall x \in X \ \forall y_1, y_2 \in Y \ (x, y_1), (x, y_2) \in f \Rightarrow y_1 = y_2$

- X: *domain*, Y: *codomain* (or *range*)
- $(x, y) \in f \equiv y = f(x)$
- y is *image* of x under f

Subset Image

Definition

subset image:

$f : X \to Y \land X_1 \subseteq X$

$f(X_1) = \{y | y \in Y, x \in X_1 \land y = f(x)\}$

Subset Image Example

Example

$f : \mathbb{R} \to \mathbb{R}$

$f(x) = x^2$

- $f(\mathbb{Z}) = \{0, 1, 4, 9, 16, \dots\}$
- $A = \{-2, 1\}$
  $f(A) = \{1, 4\}$

One-to-one Function

Definition

$f : X \to Y$ is one-to-one:

$\forall x_1, x_2 \in X \ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

One-to-one Function Examples

Example

$f : \mathbb{R} \to \mathbb{R}$
$f(x) = 3x + 7$

$$\begin{array}{rcl} & f(x_1) & = & f(x_2) \\ \Rightarrow & 3x_1 + 7 & = & 3x_2 + 7 \\ \Rightarrow & 3x_1 & = & 3x_2 \\ \Rightarrow & x_1 & = & x_2 \end{array}$$

Counterexample

$g : \mathbb{Z} \to \mathbb{Z}$
$g(x) = x^4 - x$

$$\begin{array}{rcccl} g(0) & = & 0^4 - 0 & = & 0 \\ g(1) & = & 1^4 - 1 & = & 0 \end{array}$$

Onto Function

Definition

$f : X \to Y$ is onto:
$\forall y \in Y \; \exists x \in X \; f(x) = y$

- $f(X) = Y$

Onto Function Examples

Example

$f : \mathbb{R} \to \mathbb{R}$
$f(x) = x^3$

Counterexample

$f : \mathbb{Z} \to \mathbb{Z}$
$f(x) = 3x + 1$

Bijective Function

Definition

$f : X \to Y$ is bijective:
f is both one-to-one and onto

Subset Image Properties

- $f : A \to B \wedge A_1, A_2 \subseteq A$:
  - $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
  - $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
  - if f is one-to-one:
    $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$

Composite Function

Definition

$f : X \to Y, g : Y \to Z$

$g \circ f : X \to Z$
$(g \circ f)(x) = g(f(x))$

- is not commutative
- is associative:
  $f \circ (g \circ h) = (f \circ g) \circ h$

Composite Function Examples

Example (commutativity)

$f : \mathbb{R} \to \mathbb{R}$
$f(x) = x^2$

$g : \mathbb{R} \to \mathbb{R}$
$g(x) = x + 5$

$g \circ f : \mathbb{R} \to \mathbb{R}$
$(g \circ f)(x) = x^2 + 5$

$f \circ g : \mathbb{R} \to \mathbb{R}$
$(f \circ g)(x) = (x + 5)^2$

Composite Function Theorems

Theorem

$f : X \to Y, g : Y \to Z$:
f is one-to-one $\wedge$ g is one-to-one $\Rightarrow$ $g \circ f$ is one-to-one

Proof.

$$\begin{array}{rrcl} & (g \circ f)(a_1) & = & (g \circ f)(a_2) \\ \Rightarrow & g(f(a_1)) & = & g(f(a_2)) \\ \Rightarrow & f(a_1) & = & f(a_2) \\ \Rightarrow & a_1 & = & a_2 \end{array}$$

$\square$

Composite Function Theorems

Theorem
$f : X \to Y, g : Y \to Z$:
f *is onto* $\wedge$ g *is onto* $\Rightarrow g \circ f$ *is onto*

Proof.
$\forall z \in Z \; \exists y \in Y \; g(y) = z$
$\forall y \in Y \; \exists x \in X \; f(x) = y$
$\Rightarrow \forall z \in Z \; \exists x \in X \; g(f(x)) = z$ □

Identity Function

Definition
identity function: 1_X

$1_X : X \to X$
$1_X(x) = x$

Inverse Function

Definition
$f : X \to Y$ is invertible:
$\exists f^{-1} : Y \to X \; f^{-1} \circ f = 1_X \wedge f \circ f^{-1} = 1_Y$

- f^{-1}: inverse of function f

Inverse Function Examples

Example
$f : \mathbb{R} \to \mathbb{R}$
$f(x) = 2x + 5$

$f^{-1} : \mathbb{R} \to \mathbb{R}$
$f^{-1}(x) = \frac{x-5}{2}$

$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(2x+5) = \frac{(2x+5)-5}{2} = \frac{2x}{2} = x$
$(f \circ f^{-1})(x) = f(f^{-1}(x)) = f(\frac{x-5}{2}) = 2\frac{x-5}{2} + 5 = (x-5) + 5 = x$

Inverse Function

Theorem
If a function is invertable, its inverse is unique.

Proof.
$f : X \to Y$

$g, h : Y \to X$
$g \circ f = 1_X \wedge f \circ g = 1_Y$
$h \circ f = 1_X \wedge f \circ h = 1_Y$

$h = h \circ 1_Y = h \circ (f \circ g) = (h \circ f) \circ g = 1_X \circ g = g$ □

Invertible Function

Theorem
A function is invertible if and only if it is one-to-one and onto.

Invertible Function

If invertible then one-to-one.
$f : A \to B$

$$\begin{aligned} & f(a_1) = f(a_2) \\ \Rightarrow\ & f^{-1}(f(a_1)) = f^{-1}(f(a_2)) \\ \Rightarrow\ & (f^{-1} \circ f)(a_1) = (f^{-1} \circ f)(a_2) \\ \Rightarrow\ & 1_A(a_1) = 1_A(a_2) \\ \Rightarrow\ & a_1 = a_2 \end{aligned}$$

□

If invertible then onto.
$f : A \to B$

$$\begin{aligned} & b \\ =\ & 1_B(b) \\ =\ & (f \circ f^{-1})(b) \\ =\ & f(f^{-1}(b)) \end{aligned}$$

□

Invertible Function

If bijective then invertible.
$f : A \to B$

- f is onto $\Rightarrow \forall b \in B\ \exists a \in A\ f(a) = b$
- let $g : B \to A$ be defined by $a = g(b)$
- is it possible that $g(b) = a_1 \neq a_2 = g(b)$?
- this would mean: $f(a_1) = b = f(a_2)$
- but: f is one-to-one

□

Permutations

- permutation: a bijective function on a set

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ p(a_1) & p(a_2) & \dots & p(a_n) \end{pmatrix}$$

- $n!$ permutations can be defined in a set of n elements

Permutation Examples

Example

$A = \{1, 2, 3\}$

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Cyclic Permutation

- *cyclic permutation*:
  - a subset of elements form a cycle
  - the remaining elements do not change

$$(a_i, a_j, a_k) = \begin{pmatrix} \dots & a_i & \dots & a_n & \dots & a_j & \dots & a_k & \dots \\ \dots & a_j & \dots & a_n & \dots & a_k & \dots & a_i & \dots \end{pmatrix}$$

- *transposition*: a cyclic permutation of length 2

Cyclic Permutation Examples

Example

$A = \{1, 2, 3, 4, 5\}$

$$(1, 3, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

Permutation Composition

- permutation composition is not commutative

Example

$A = \{1, 2, 3, 4, 5\}$

$$
\begin{aligned}
(4,1,3,5) \diamond (5,2,3) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \diamond \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} \\
(5,2,3) \diamond (4,1,3,5) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \diamond \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}
\end{aligned}
$$

Cyclic Permutation Composition

- all permutations that are not cyclic can be written as a composition of disjoint cyclic permutations

Example

$A = \{1, 2, 3, 4, 5, 6, 7, 8\}$

$$
\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 5 & 2 & 1 & 8 & 7 \end{pmatrix} = (1,3,6) \diamond (2,4,5) \diamond (7,8)
$$

Transposition Composition

- all cyclic permutations can be written as a composition of transpositions

Example

$A = \{1, 2, 3, 4, 5\}$

$(1,2,3,4,5) = (1,2) \diamond (1,3) \diamond (1,4) \diamond (1,5)$

Pigeonhole Principle

Definition

pigeonhole principle (Dirichlet drawers):
if m pigeons go into n holes and $m > n$
at least one hole contains more than one pigeon

- if $f : X \to Y \wedge |X| > |Y|$ then f cannot be one-to-one
- $\exists x_1, x_2 \in X \; x_1 \neq x_2 \wedge f(x_1) = f(x_2)$

Pigeonhole Principle Examples

Example

- In a room where there are 367 people, at least two persons have the same birthday.
- How many students should take an exam where the grades are between 0 and 100 so that two students have the same grade?

Generalized Pigeonhole Principle

Definition

generalized pigeonhole principle:
if m objects are distributed to n drawers
at least one of the drawers contains $\lceil m/n \rceil$ objects

Example

In a room where there are 100 people at least $\lceil 100/12 \rceil = 9$ persons were born in the same month.

Pigeonhole Principle Example

Theorem

There are two elements which total 10 in any subset of cardinality 6 of the set $S = \{1,2,3,\ldots,9\}$.

Pigeonhole Principle Example

Theorem

Let S be a set of positive integers smaller than or equal to 14, with cardinality 6. The sums of the elements in all nonempty subsets of S cannot be all different.

Proof Trial

$A \subseteq S$
s_A : sum of the elements of A

- holes: $1 \leq s_A \leq 9 + \cdots + 14 = 69$
- pigeons: $2^6 - 1 = 63$

Proof.

look at the subsets for which $|A| \leq 5$

- holes: $1 \leq s_A \leq 10 + \cdots + 14 = 60$
- pigeons: $2^6 - 2 = 62$

□

Pigeonhole Principle Example

Theorem
There is at least one pair of elements among 101 elements chosen from set $S = \{1, 2, 3, \ldots, 200\}$ *so that one of the elements of the pair divides the other.*

Proof Method

- we first show that $\forall n\ \exists! p\ (n = 2^r p \wedge r \geq 0 \wedge \exists t \in \mathbb{Z}\ p = 2t + 1)$
- then, by using this theorem we prove the main theorem

Pigeonhole Principle Example

Theorem
$\forall n\ \exists! p\ (n = 2^r p \wedge r \geq 0 \wedge \exists t \in \mathbb{Z}\ p = 2t + 1)$

Proof of Existence.
$n = 1$: $r = 0, p = 1$
$n = 2$: $r = 1, p = 1$
$n \leq k$: $n = 2^r p$
$n = k + 1$:

$$\begin{array}{ll} n\ \textit{prime}: & r = 0, p = n \\ \neg(n\ \textit{prime}): & n = n_1 n_2 \\ & n = 2^{r_1} p_1 \cdot 2^{r_2} p_2 \\ & n = 2^{r_1 + r_2} \cdot p_1 p_2 \end{array}$$

$\square$

Proof of Uniqueness.
if not unique:

$$\begin{array}{rcccl} n & = & 2^{r_1} p_1 & = & 2^{r_2} p_2 \\ & \Rightarrow & 2^{r_1 - r_2} p_1 & = & p_2 \\ & \Rightarrow & 2 | p_2 & & \end{array}$$

$\square$

Pigeonhole Principle Example

Theorem
There is at least one pair of elements among 101 elements chosen from set $S = \{1, 2, 3, \ldots, 200\}$ *so that one of the elements of the pair divides the other.*

Proof.

- $T \subseteq S$, Assume that T is a subset of S that contains all odd elements of S: $|T| = 100$
- $f : S \to T, (s, t) \in f \equiv s = 2^r t \wedge r \geq 0$
  - if 101 elements are chosen from S, at least two of them will have the same image in T: $f(s_1) = f(s_2) \Rightarrow 2^{m_1} t = 2^{m_2} t$

$$\frac{s_1}{s_2} = \frac{2^{m_1} t}{2^{m_2} t} = 2^{m_1 - m_2}$$

$\square$

Recursive Functions

Definition
recursive function:
a function defined in terms of itself

$f(n) = h(f(m))$

- *inductively defined function*:
  the size reduced at every step of the recursion

$$f(n) = \begin{cases} k & n = 0 \\ h(f(n-1)) & n > 0 \end{cases}$$

Recursive Function Examples

Example

$$f91(n) = \begin{cases} n - 10 & n > 100 \\ f91(f91(n+11)) & n \leq 100 \end{cases}$$

Inductively Defined Function Examples

Example (factorial)

$$f(n) = \begin{cases} 1 & n = 0 \\ n \cdot f(n-1) & n > 0 \end{cases}$$

Example (function power)

$$f^n = \begin{cases} f & n = 1 \\ f \circ f^{n-1} & n > 1 \end{cases}$$

Euclid Algorithm

Example (greatest common divisor)

$$\begin{aligned} 333 &= 3 \cdot 84 + 81 \\ 84 &= 1 \cdot 81 + 3 \\ 81 &= 27 \cdot 3 + 0 \end{aligned}$$

$gcd(333, 84) = 3$

$$gcd(a, b) = \begin{cases} b & b | a \\ gcd(b, a \ mod \ b) & b \nmid a \end{cases}$$

Fibonacci Series

Fibonacci series

$$F_n = fib(n) = \begin{cases} 1 & n = 1 \\ 1 & n = 2 \\ fib(n-1) + fib(n-2) & n > 2 \end{cases}$$

F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	...
1	1	2	3	5	8	13	21	...

Fibonacci Series

Theorem

$\sum_{i=1}^{n} {F_i}^2 = F_n \cdot F_{n+1}$

Proof.

$$
\begin{array}{lrcl}
n = 2: & \sum_{i=1}^{2} {F_i}^2 & = & {F_1}^2 + {F_2}^2 = 1 + 1 = 1 \cdot 2 = F_2 \cdot F_3 \\
n = k: & \sum_{i=1}^{k} {F_i}^2 & = & F_k \cdot F_{k+1} \\
n = k+1: & \sum_{i=1}^{k+1} {F_i}^2 & = & \sum_{i=1}^{k} {F_i}^2 + {F_{k+1}}^2 \\
 & & = & F_k \cdot F_{k+1} + {F_{k+1}}^2 \\
 & & = & F_{k+1} \cdot (F_k + F_{k+1}) \\
 & & = & F_{k+1} \cdot F_{k+2}
\end{array}
$$

□

Ackermann Function

Ackermann function

$$
ack(x, y) = \begin{cases} y + 1 & x = 0 \\ ack(x-1, 1) & y = 0 \\ ack(x-1, ack(x, y-1)) & x > 0 \land y > 0 \end{cases}
$$

References

Required Text: Grimaldi

- Chapter 5: Relations and Functions
  - 5.2. Functions: Plain and One-to-One
  - 5.3. Onto Functions: Stirling Numbers of the Second Kind
  - 5.5. The Pigeonhole Principle
  - 5.6. Function Composition and Inverse Functions

Supplementary Text: O'Donnell, Hall, Page

- Chapter 11: Functions