Discrete Mathematics

Relations and Functions

H. Turgut Uyar   Ayşegül Gençata Yayımlı   Emre Harmancı

2001-2014

License

Topics

Relation

Definition

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

- tuple: an element of a relation

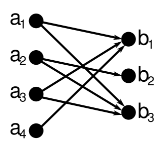
- $\alpha \subseteq A \times B$: *binary relation*
- $a \alpha b$ is the same as $(a, b) \in \alpha$

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

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

Relation Composition

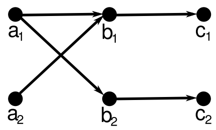
Definition

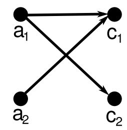
relation composition:

let $\alpha \subseteq A \times B$, $\beta \subseteq B \times C$

$\alpha\beta = \{(a, c) \mid a \in A, c \in C, \exists b \in B\ [a\alpha b \wedge b\beta c]\}$

Example





Relation Composition

- $M_{\alpha\beta} = M_\alpha \times M_\beta$
- using logical operations:
  $1 : T \quad 0 : F \quad \cdot : \wedge \quad + : \vee$

Example

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

Relation Composition Associativity

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

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

□

Relation Composition Theorems

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

Relation Composition Theorems

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

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

□

Converse Relation

Definition
$\alpha^{-1} = \{(b, a) \mid (a, b) \in \alpha\}$

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

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

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

$$
\begin{aligned}
& (b, a) \in \overline{\alpha}^{-1} \\
\Leftrightarrow \quad & (a, b) \in \overline{\alpha} \\
\Leftrightarrow \quad & (a, b) \notin \alpha \\
\Leftrightarrow \quad & (b, a) \notin \alpha^{-1} \\
\Leftrightarrow \quad & (b, a) \in \overline{\alpha^{-1}}
\end{aligned}
$$

□

Converse Relation Theorems

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

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

□

Converse Relation Theorems

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

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

□

Relation Composition Converse

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

Proof.

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

□

Relation Properties

- let $\alpha \subseteq A \times A$
- α^n: $\alpha\alpha\cdots\alpha$
- identity relation: $E = \{(a, a) \mid a \in A\}$

Reflexivity

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

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

Reflexivity Examples

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

- $\mathcal{R}_1$ is reflexive

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

- $\mathcal{R}_2$ 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

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

- $\mathcal{R}$ is reflexive

Symmetry

symmetric

$\alpha \subseteq A \times A$
$\forall a, b\ [(a = b) \vee (a\alpha b \wedge b\alpha a) \vee (\neg(a\alpha b) \wedge \neg(b\alpha a))]$
$\forall a, b\ [(a = b) \vee (a\alpha b \leftrightarrow b\alpha a)]$

- $\alpha^{-1} = \alpha$
- 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:

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

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

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

- $\mathcal{R}$ is symmetric

Symmetry Examples

Example

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

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

Transitivity

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

- $\alpha^2 \subseteq \alpha$
- 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

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

- $\mathcal{R}$ is nontransitive

Converse Relation Properties

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

Closures

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

Special Relations

predecessor - successor

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

- irreflexive
- antisymmetric
- antitransitive

Special Relations

adjacency

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

- irreflexive
- symmetric
- antitransitive

Special Relations

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

- irreflexive
- antisymmetric
- transitive

Special Relations

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

- reflexive
- antisymmetric
- transitive

Special Relations

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

- reflexive
- asymmetric
- transitive

Special Relations

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

- reflexive
- symmetric
- nontransitive

Special Relations

comparability

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

$\mathcal{R} = \{(a, b) \mid (a \subseteq b) \vee (b \subseteq a)\}$

- reflexive
- symmetric
- nontransitive

Special Relations

sibling

- irreflexive
- symmetric
- transitive

- can a relation be symmetric, transitive and irreflexive?

Compatibility Relations

Definition

compatibility relation: γ

- reflexive
- symmetric

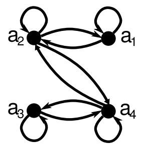
- when drawing, lines instead of arrows
- matrix representation as a triangle matrix

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

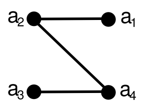
Compatibility Relation Example

Example

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



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



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

Compatibility Relation Example

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

P: persons, L: languages
$P = \{p_1, p_2, p_3, p_4, p_5, p_6\}$
$L = \{l_1, l_2, l_3, l_4, l_5\}$

$\alpha \subseteq P \times L$

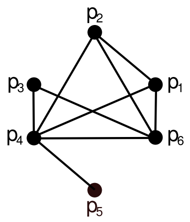
$$M_\alpha = \begin{vmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{vmatrix} \qquad M_{\alpha^{-1}} = \begin{vmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 &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

Compatibility Relation Example

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

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

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



Compatibility Block

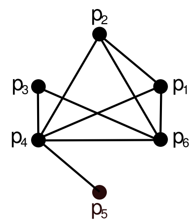
Definition

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

Compatibility Block Example

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



- $C_1 = \{p_4, p_6\}$
- $C_2 = \{p_2, p_4, p_6\}$
- $C_3 = \{p_1, p_2, p_4, p_6\}$ (MCB)

$$C_\gamma = \{\{p_1, p_2, p_4, p_6\}, \{p_3, p_4, p_6\}, \{p_4, p_5\}\}$$

Equivalence Relations

Definition

equivalence relation: ϵ

- reflexive
- symmetric
- transitive

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

- complete cover: C_ϵ

Equivalence Relation Example

Example

$\mathcal{R} \subseteq \mathbb{Z} \times \mathbb{Z}$
$\mathcal{R} = \{(a, b) \mid \exists m \in \mathbb{Z}\ [a - b = 5m]\}$

- $\mathcal{R}$ partitions $\mathbb{Z}$ into 5 equivalence classes

References

Required Reading: 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 Reading: O'Donnell, Hall, Page

- Chapter 10: Relations

Functions

Definition

function: $f : X \to Y$
$\forall x \in X\ \forall y_1, y_2 \in Y\ [(x, y_1), (x, y_2) \in f \to y_1 = y_2]$

- X: domain, Y: codomain (or *range*)

- $y = f(x)$ is the same as $(x, y) \in f$
- y is the *image* of x under f

- let $f : X \to Y$ and $X_1 \subseteq X$
  subset image: $f(X_1) = \{f(x) \mid x \in X_1\}$

Subset Image Examples

Example

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

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

$f(\{-2, 1\}) = \{1, 4\}$

Function Properties

Definition

$f : X \to Y$ is one-to-one (or injective):
$\forall x_1, x_2 \in X\ [f(x_1) = f(x_2) \to x_1 = x_2]$

Definition

$f : X \to Y$ is onto (or surjective):
$\forall y \in Y\ \exists x \in X\ [f(x) = y]$

- $f(X) = Y$

Definition

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

One-to-one Function Examples

Example

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

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

Counterexample

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

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

Onto Function Examples

Example

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

Counterexample

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

Function Composition

Definition

let $f : X \to Y$ and $g : Y \to Z$

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

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

Function Composition 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

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

Proof.

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

□

Composite Function Theorems

Theorem

let $f : X \to Y$ and $g : Y \to Z$
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 invertible, its inverse is unique.

Proof.
let $f : X \to Y$

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

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

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

□

Pigeonhole Principle

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

- let $f : X \to Y$
  $|X| > |Y| \Rightarrow f$ is not 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

- Among 367 people, at least two have the same birthday.
- In an exam where the grades are integers between 0 and 100, how many students have to take the exam to make sure that at least two students will have the same grade?

Generalized Pigeonhole Principle

Definition

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

Example

Among 100 people, at least 9 ($\lceil 100/12 \rceil$) were born in the same month.

Pigeonhole Principle Example

Theorem

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

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

Among any 101 elements chosen from the set $S = \{1, 2, 3, \ldots, 200\}$ there are at least two numbers such that one divides the other.

Proof Method

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

Pigeonhole Principle Example

Theorem

$\forall n \; \exists! p \; [n = 2^r p \wedge r \in \mathbb{N} \wedge \exists t \in \mathbb{Z} \; [p = 2t + 1]]$

Proof of existence.

$n = 1$: $r = 0, p = 1$

$n \leq k$: assume $n = 2^r p$

$n = k + 1$:

$$\begin{array}{ll} n = 2: & r = 1, p = 1 \\ n \text{ prime } (n > 2): & r = 0, p = n \\ \neg(n \text{ prime}): & n = n_1 n_2 \\ & n = 2^{r_1} p_1 \cdot 2^{r_2} p_2 \\ & n = 2^{r_1 + r_2} \cdot p_1 p_2 \end{array}$$

$\square$

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

Among any 101 elements chosen from the set $S = \{1, 2, 3, \ldots, 200\}$ there are at least two numbers such that one divides the other.

Proof.

- $T = \{t \mid t \in S, \exists i \in \mathbb{Z} \; [t = 2i + 1]\}$, $|T| = 100$
- let $f : S \to T$ and $r \in \mathbb{N}$
  $s = 2^r t \to f(s) = t$
  - 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*: a recursive function where the size is reduced at every step

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

Recursion Examples

Example

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

Example (factorial)

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

Euclid Algorithm

Example (greatest common divisor)

$$gcd(a,b) = \begin{cases} b & \text{if } b \mid a \\ gcd(b, a \; mod \; b) & \text{if } b \nmid a \end{cases}$$

$$\begin{aligned} gcd(333, 84) &= gcd(84, 333 \; mod \; 84) \\ &= gcd(84, 81) \\ &= gcd(81, 84 \; mod \; 81) \\ &= gcd(81, 3) \\ &= 3 \end{aligned}$$

Fibonacci Sequence

Fibonacci sequence

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

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 Sequence

Theorem

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

Proof.

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

$\square$

Ackermann Function

Ackermann function

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

References

Required Reading: 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 Reading: O'Donnell, Hall, Page

- Chapter 11: Functions