Discrete Mathematics

Relations and Functions

H. Turgut Uyar   Ayşegül Gençata Yayımlı   Emre Harmancı

2001-2023

License

Topics

Relation

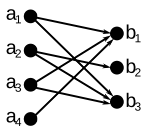
Definition

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

- tuple: element of relation
- *binary* relation: $\alpha \subseteq A \times B$
- $a \alpha b \quad : \quad (a, b) \in \alpha$

Relation Example

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



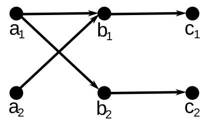
$$M_\alpha = \begin{array}{c c} & \begin{array}{ccc} b_1 & b_2 & b_3 \end{array} \\ \begin{array}{c} a_1 \\ a_2 \\ a_3 \\ a_4 \end{array} & \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

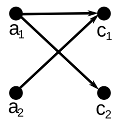
Relation Composition

Definition

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

example





Relation Composition

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

example

$$M_\alpha = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \quad M_\beta = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad M_{\alpha\beta} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

Relation Composition Associativity

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

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

$\square$

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

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

Converse Relation Theorems

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

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

□

Converse Relation Theorems

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

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

□

Converse Relation Theorems

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

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

□

Relation Composition Converse

Theorem

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

Proof.

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

□

Relation Properties

- $\alpha \subseteq A \times A$
- α^2: $\alpha\alpha$
- α^n: $\alpha\alpha\cdots\alpha$
- identity relation: $E = \{(a, a) \mid a \in A\}$

Reflexivity

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

- $E \subseteq \alpha$
- irreflexive:
  $\forall a \in A\ [\neg(a \alpha a)]$

Reflexivity Examples

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

- $\mathcal{R}_1$ is reflexive

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

- $\mathcal{R}_2$ is not reflexive
- also not irreflexive

Reflexivity Examples

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

- $\mathcal{R}$ is irreflexive

Reflexivity Examples

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

- $\mathcal{R}$ is reflexive

Symmetry

symmetric

$\alpha \subseteq A \times A$

$\forall a, b \in A \; [a\alpha b \leftrightarrow b\alpha a]$

- $\alpha^{-1} = \alpha$
- antisymmetric:
  $\forall a, b \in A \; [a\alpha b \wedge b\alpha a \rightarrow a = b]$

Symmetry Examples

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

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

- $\mathcal{R}$ is not symmetric
- also not antisymmetric

Symmetry Examples

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

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

- $\mathcal{R}$ is symmetric

Symmetry Examples

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

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

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

Transitivity

transitive

$\alpha \subseteq A \times A$

$\forall a, b, c \in A \; [a\alpha b \wedge b\alpha c \rightarrow a\alpha c]$

- $\alpha^2 \subseteq \alpha$
- antitransitive:
  $\forall a, b, c \in A \; [a\alpha b \wedge b\alpha c \rightarrow \neg(a\alpha c)]$

Transitivity Examples

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

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

- $\mathcal{R}$ is antitransitive

Transitivity Examples

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

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

- $\mathcal{R}$ is not transitive
- also not antitransitive

Converse Relation Properties

Theorem

Reflexivity, symmetry, and transitivity are preserved in the converse relation.

Closures

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

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
- 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

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

Special Relations

- siblings?
- irreflexive
- symmetric
- transitive
- can a relation be symmetric and transitive, but irreflexive?

Compatibility Relations

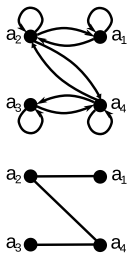
Definition

compatibility relation: γ

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

Compatibility Relation Example

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



Compatibility Relation Example

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

$$
\begin{array}{c} \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{array}
\begin{array}{c} \begin{array}{cccc} a_1 & a_2 & a_3 & a_4 \end{array} \\
\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \end{array}
$$

$$
\begin{array}{c} \\ a_2 \\ a_3 \\ a_4 \end{array}
\begin{array}{c} \begin{array}{ccc} a_1 & a_2 & a_3 \end{array} \\
\begin{bmatrix} 1 & & \\ 0 & 0 & \\ 0 & 1 & 1 \end{bmatrix} \end{array}
$$

Compatibility Relations

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

example

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

Compatibility Relation Example

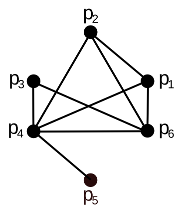
$$M_\alpha = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \end{array} \begin{array}{c} \begin{array}{ccccc} l_1 & l_2 & l_3 & l_4 & l_5 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

$$M_{\alpha^{-1}} = \begin{array}{c} \\ l_1 \\ l_2 \\ l_3 \\ l_4 \\ l_5 \end{array} \begin{array}{c} \begin{array}{cccccc} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Compatibility Relation Example

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

$$M_{\alpha\alpha^{-1}} = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \end{array} \begin{array}{c} \begin{array}{cccccc} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

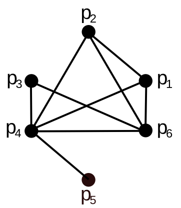


Compatibility Block

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



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

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

- $\mathcal{R}$ 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

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
- $y = f(x) \quad : \quad (x, y) \in f$
- y: *image* of x under f
- $f : X \to Y$, $X' \subseteq X$
  subset image: $f(X') = \{f(x) \mid x \in X'\}$

Subset Image Examples

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

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

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

Range

Definition

$f : X \to Y$

range: $f(X)$

One-to-One Functions

Definition

$f : X \to Y$ is one-to-one (or injective):

$\forall x_1, x_2 \in X \ [f(x_1) = f(x_2) \to x_1 = x_2]$

One-to-One Function Examples

- one-to-one

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

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

- not one-to-one

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

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

Onto Functions

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

- $f(X) = Y$

Onto Function Examples

- onto

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

- not onto

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

Bijective Functions

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

Function Composition

Definition

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

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

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

Composition Commutativity Example

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

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

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

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

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.

$$\begin{array}{rrcl} & (g \circ f)(x_1) & = & (g \circ f)(x_2) \\ \Rightarrow & g(f(x_1)) & = & g(f(x_2)) \\ \Rightarrow & f(x_1) & = & f(x_2) \\ \Rightarrow & x_1 & = & x_2 \end{array}$$

$\square$

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.

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

$\square$

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

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

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

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

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

Inverse Function

Theorem

If a function is invertible, its inverse is unique.

Proof.

$f : X \to Y$

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

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

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.
$f : X \to Y$

$$\begin{aligned} & f(x_1) = f(x_2) \\ \Rightarrow\ & f^{-1}(f(x_1)) = f^{-1}(f(x_2)) \\ \Rightarrow\ & (f^{-1} \circ f)(x_1) = (f^{-1} \circ f)(x_2) \\ \Rightarrow\ & 1_X(x_1) = 1_X(x_2) \\ \Rightarrow\ & x_1 = x_2 \end{aligned}$$

□

If invertible then onto.
$f : X \to Y$

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

□

Invertible Function

If bijective then invertible.
$f : X \to Y$

- f is onto $\Rightarrow \forall y \in Y\ \exists x \in X\ f(x) = y$
- let $g : Y \to X$ be defined by $x = g(y)$
- is it possible that $g(y) = x_1 \neq x_2 = g(y)$?
- this would mean: $f(x_1) = y = f(x_2)$
- 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.

- $f : X \to Y$
  $|X| > |Y| \Rightarrow f$ 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

- 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 $\lceil 100/12 \rceil = 9$ were born in the same month.

Pigeonhole Principle Example

Theorem

$S = \{1, 2, 3, \ldots, 9\}, T \subset S, |T| = 6$
$\exists s_1, s_2 \in T\ [s_1 + s_2 = 10]$

Pigeonhole Principle Example

Theorem

$S \subseteq \mathbb{Z}^+$, $\forall a \in S\ [a \leq 14]$, $|S| = 6$
$T = \mathcal{P}(S) - \emptyset$
$X = \{\Sigma_A \mid A \in T\}$, Σ_A : *sum of the elements in A*
$|X| < |T|$

Proof Attempt

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

Proof.

consider $T - S$

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

□

Pigeonhole Principle Example

Theorem

$S = \{1, 2, 3, \ldots, 200\}, T \subset S, |T| = 101$

$\exists s_1, s_2 \in T\ [s_2 | s_1]$

- 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, use this to 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 $n = 2^r p$

$n = k + 1$:

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

□

Proof of uniqueness.

if not unique:

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

□

Pigeonhole Principle Example

Theorem

$S = \{1, 2, 3, \ldots, 200\}, T \subset S, |T| = 101$

$\exists s_1, s_2 \in T\ [s_2 | s_1]$

Proof.

- $P = \{p \mid p \in S, \exists i \in \mathbb{Z}\ [p = 2i + 1]\}, |P| = 100$
- $f : S \to P, r \in \mathbb{N}, s = 2^r p \to f(s) = p$
- $|T| = 101 \Rightarrow$ at least two elements have the same image in P: $f(s_1) = f(s_2) \Rightarrow s_1 = 2^{r_1} p, s_2 = 2^{r_2} p$

$$\frac{s_1}{s_2} = \frac{2^{r_1} p}{2^{r_2} p} = 2^{r_1 - r_2}$$

□

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

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

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

Greatest Common Divisor

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

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

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

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

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