Week 4-5: Binary Relations

1 Binary Relations

The concept of relation is common in daily life and seems intuitively clear. For instance, let X denote the set of all females and Y the set of all males. The wife-husband relation R can be thought as a relation from X to Y. For a lady $x \in X$ and a gentleman $y \in Y$, we say that x is related to y by R if x is a wife of y, written as xRy. To describe the relation R, we may list the collection of all ordered pairs (x, y) such that x is related to y by R. The collection of all such related ordered pairs is simply a subset of the Cartesian product $X \times Y$. This motivates the following definition of binary relations.

Definition 1.1. Let X and Y be nonempty sets. A **binary relation** from X to Y is a subset

$$R \subseteq X \times Y.$$

If $(x, y) \in R$, we say that x is related to y by R, denoted xRy. If $(x, y) \notin R$, we say that x is not related to y, denoted $x\bar{R}y$. For each element $x \in X$, we denote by $R(x)$ the subset of elements of Y that are related to x, that is,

$$R(x) = \{y \in Y : xRy\} = \{y \in Y : (x, y) \in R\}.$$

For each subset $A \subseteq X$, we define

$$R(A) = \{y \in Y : \exists\ x \in A \text{ such that } xRy\} = \bigcup_{x \in A} R(x).$$

When $X = Y$, we say that R is a **binary relation on** X.

Since binary relations from X to Y are subsets of $X \times Y$, we can define intersection, union, and complement for binary relations. The **complementary relation** of a binary relation $R \subseteq X \times Y$ is the binary relation $\bar{R} \subseteq X \times Y$ defined by

$$x\bar{R}y \iff (x, y) \notin R.$$

The **converse relation** (or **reverse relation**) of R is the binary relation $R^{-1} \subseteq Y \times X$ defined by

$$yR^{-1}x \ \Leftrightarrow (x, y) \in R.$$

Example 1.1. Consider a family A with five children, Amy, Bob, Charlie, Debbie, and Eric. We abbreviate the names to their first letters so that

$$A = \{a, b, c, d, e\}.$$

(a) The brother-sister relation R_{bs} is the set

$$R_{bs} = \{(b, a), (b, d), (c, a), (c, d), (e, a), (e, d)\}.$$

(b) The sister-brother relation R_{sb} is the set

$$R_{sb} = \{(a, b), (a, c), (a, e), (d, b), (d, c), (d, e)\}.$$

(c) The brother relation R_b is the set

$$\{(b, b), (b, c), (b, e), (c, b), (c, c), (c, e), (e, b), (e, c), (e, e)\}.$$

(d) The sister relation R_s is the set

$$\{(a, a), (a, d), (d, a), (d, d)\}.$$

The brother-sister relation R_{bs} is the inverse of the sister-brother relation R_{sb}, i.e.,

$$R_{bs} = R_{sb}^{-1}.$$

The brother or sister relation is the union of the brother relation and the sister relation, i.e.,

$$R_b \cup R_s.$$

The complementary relation of the brother or sister relation is the brother-sister or sister-brother relation, i.e.,

$$\overline{R_b \cup R_s} = R_{bs} \cup R_{sb}.$$

Example 1.2. (a) The graph of equation

$$\frac{x^2}{3^2} + \frac{y^2}{2^2} = 1$$

is a binary relation on $\mathbb{R}$. The graph is an ellipse.

(b) The relation less than, denoted by $<$, is a binary relation on $\mathbb{R}$ defined by

$$a < b \quad \text{if } a \text{ is less than } b.$$

As a subset of $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, the relation is given by the set

$$\{(a, b) \in \mathbb{R}^2 : a \text{ is less than } b\}.$$

(c) The relation greater than or equal to is a binary relation $\geq$ on $\mathbb{R}$ defined by

$$a \geq b \quad \text{if } a \text{ is greater than or equal to } b.$$

As a subset of $\mathbb{R}^2$, the relation is given by the set

$$\{(a, b) \in \mathbb{R}^2 : a \text{ is greater than or equal to } b\}.$$

(d) The divisibility relation $\mid$ about integers, defined by

$$a \mid b \quad \text{if } a \text{ divides } b,$$

is a binary relation on the set $\mathbb{Z}$ of integers. As a subset of $\mathbb{Z}^2$, the relation is given by

$$\{(a, b) \in \mathbb{Z}^2 : a \text{ is a factor of } b\}.$$

Example 1.3. Any function $f : X \to Y$ can be viewed as a binary relation from X to Y. The binary relation is just its graph

$$G(f) = \{(x, f(x)) : x \in X\} \subseteq X \times Y.$$

Proposition 1.2. *Let $R \subseteq X \times Y$ be a binary relation from X to Y. Let $A, B \subseteq X$ be subsets.*

(a) If $A \subseteq B$, then $R(A) \subseteq R(B)$.

(b) $R(A \cup B) = R(A) \cup R(B)$.

(c) $R(A \cap B) \subseteq R(A) \cap R(B)$.

Proof. (a) For any $y \in R(A)$, there is an $x \in A$ such that xRy. Since $A \subseteq B$, then $x \in B$. Thus $y \in R(B)$. This means that $R(A) \subseteq R(B)$.

(b) For any $y \in R(A \cup B)$, there is an $x \in A \cup B$ such that xRy. If $x \in A$, then $y \in R(A)$. If $x \in B$, then $y \in R(B)$. In either case, $y \in R(A) \cup R(B)$. Thus

$$R(A \cup B) \subseteq R(A) \cup R(B).$$

On the other hand, it follows from (a) that

$$R(A) \subseteq R(A \cup B) \quad \text{and} \quad R(B) \subseteq R(A \cup B).$$

Thus $R(A) \cup R(B) \subseteq R(A \cup B)$.

(c) It follows from (a) that

$$R(A \cap B) \subseteq R(A) \quad \text{and} \quad R(A \cap B) \subseteq R(B).$$

Thus $R(A \cap B) \subseteq R(A) \cap R(B)$. $\square$

Proposition 1.3. *Let $R_1, R_2 \subseteq X \times Y$ be relations from X to Y. If $R_1(x) = R_2(x)$ for all $x \in X$, then $R_1 = R_2$.*

Proof. If xR_1y, then $y \in R_1(x)$. Since $R_1(x) = R_2(x)$, we have $y \in R_2(x)$. Thus xR_2y. A similar argument shows that if xR_2y then xR_1y. Therefore $R_1 = R_2$. $\square$

2 Representation of Relations

Binary relations are the most important relations among all relations. Ternary relations, quaternary relations, and multi-factor relations can be studied by binary relations. There are two ways to represent a binary relation, one by a directed graph and the other by a matrix.

Let R be a binary relation on a finite set $V = \{v_1, v_2, \ldots, v_n\}$. We may describe the relation R by drawing a directed graph as follows: For each element $v_i \in V$, we draw a solid dot and name it by v_i; the dot is called a **vertex**. For two vertices v_i and v_j, if v_iRv_j, we draw an arrow from v_i to v_j, called a **directed edge**. When $v_i = v_j$, the directed edge becomes a **directed loop**.

The resulted graph is a directed graph, called the **digraph** of R, and is denoted by $D(R)$. Sometimes the directed edges of a digraph may have to cross each other when drawing the digraph on a plane. However, the intersection points of directed edges are not considered to be vertices of the digraph.

The **in-degree** of a vertex $v \in V$ is the number of vertices u such that uRv, and is denoted by

$$\text{indeg}\,(v).$$

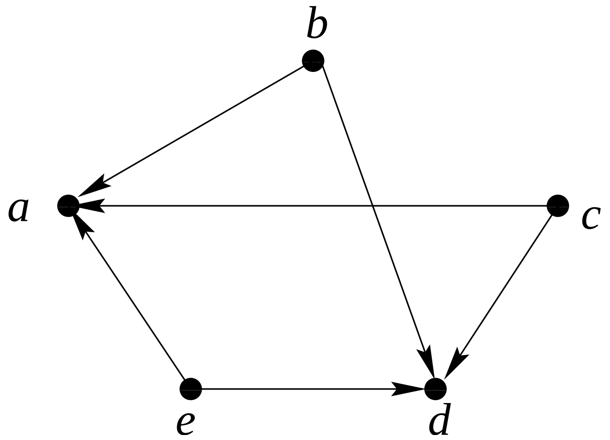
The **out-degree** of v is the number of vertices w such that vRw, and is denoted by

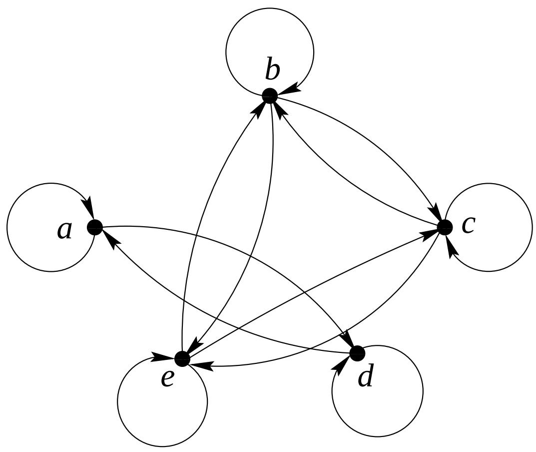
$$\text{outdeg}\,(v).$$

If $R \subseteq X \times Y$ is a relation from X to Y, we define

$$\begin{array}{rcll} \text{outdeg}\,(x) & = & |R(x)| & \text{for} \quad x \in X, \\ \text{indeg}\,(y) & = & |R^{-1}(y)| & \text{for} \quad y \in Y. \end{array}$$

The digraphs of the brother-sister relation R_{bs} and the brother or sister relation $R_b \cup R_s$ are demonstrated in the following.





Definition 2.1. Let $R \subseteq X \times Y$ be a binary relation from X to Y, where

$$X = \{x_1, x_2, \ldots, x_m\}, \quad Y = \{y_1, y_2, \ldots, y_n\}.$$

The **matrix** of the relation R is an $m \times n$ matrix $M_R = [a_{ij}]$, whose (i, j)-entry is given by

$$a_{ij} = \begin{cases} 1 & \text{if} \quad x_i R y_j \\ 0 & \text{if} \quad x_i \overline{R} y_j. \end{cases}$$

The matrix M_R is called the **Boolean matrix** of R. If $X = Y$, then $m = n$, and the matrix M_R is a square matrix.

Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be $m \times n$ Boolean matrices. If $a_{ij} \leq b_{ij}$ for all (i, j)-entries, we write $A \leq B$.

The matrix of the **brother-sister** relation R_{bs} on the set $A = \{a, b, c, d, e\}$ is the square matrix

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

and the matrix of the **brother or sister** relation is the square matrix

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

Proposition 2.2. *For any digraph $D(R)$ of a binary relation $R \subseteq V \times V$ on V,*

$$\sum_{v \in V} \text{indeg}\,(v) = \sum_{v \in V} \text{outdeg}\,(v) = |R|.$$

If R is a binary relation from X to Y, then

$$\sum_{x \in X} \text{outdeg}\,(x) = \sum_{y \in Y} \text{indeg}\,(y) = |R|.$$

Proof. Trivial. $\square$

Let R be a relation on a set X. A **directed path of length** k from x to y is a finite sequence x_0, x_1, …, x_k (not necessarily distinct), beginning with $x_0 = x$ and ending with $x_k = y$, such that

$$x_0 R x_1, \ x_1 R x_2, \ \ldots, \ x_{k-1} R x_k.$$

A path that begins and ends at the same vertex is called a **directed cycle**.

For any fixed positive integer k, let $R^k \subseteq X \times X$ denote the relation on X given by

$$xR^k y \ \Leftrightarrow\ \exists \text{ a path of length } k \text{ from } x \text{ to } y.$$

Let $R^\infty \subseteq X \times X$ denote the relation on X given by

$$xR^\infty y \ \Leftrightarrow\ \exists \text{ a directed path from } x \text{ to } y.$$

The relation R^∞ is called the **connectivity relation** for R. Clearly, we have

$$R^\infty = R \cup R^2 \cup R^3 \cup \cdots = \bigcup_{k=1}^{\infty} R^k.$$

The **reachability relation** of R is the binary relation $R^* \subseteq X \times X$ on X defined by

$$xR^* y \ \Leftrightarrow\ x = y \ \text{ or } \ xR^\infty y.$$

Obviously,

$$R^* = I \cup R \cup R^2 \cup R^3 \cup \cdots = \bigcup_{k=0}^{\infty} R^k,$$

where I is the identity relation on X defined by

$$xIy \quad \Leftrightarrow \quad x = y.$$

We always assume that $R^0 = I$ for any relation R on a set X.

Example 2.1. Let $X = \{x_1, \ldots, x_n\}$ and $R = \{(x_i, x_{i+1}) : i = 1, \ldots, n-1\}$. Then

$$R^k = \{(x_i, x_{i+k}) : i = 1, \ldots, n-k\}, \quad 1 \le k \le n/2;$$
$$R^k = \varnothing, \quad k \ge (n+1)/2;$$
$$R^\infty = \{(x_i, x_j) : i < j\}.$$

If $R = \{(x_i, x_{i+1}) : i = 1, \ldots, n\}$ with $x_{n+1} = x_1$, then $R^\infty = X \times X = X^2$.

3 Composition of Relations

Definition 3.1. Let $R \subseteq X \times Y$ and $S \subseteq Y \times Z$ binary relations. The **composition** of R and S is a binary relation $S \circ R \subseteq X \times Z$ from X to Z

defined by

$$x(S \circ R)z \;\Leftrightarrow\; \exists\, y \in Y \text{ such that } xRy \text{ and } ySz.$$

When $X = Y$, the relation R is a binary relation on X. We have

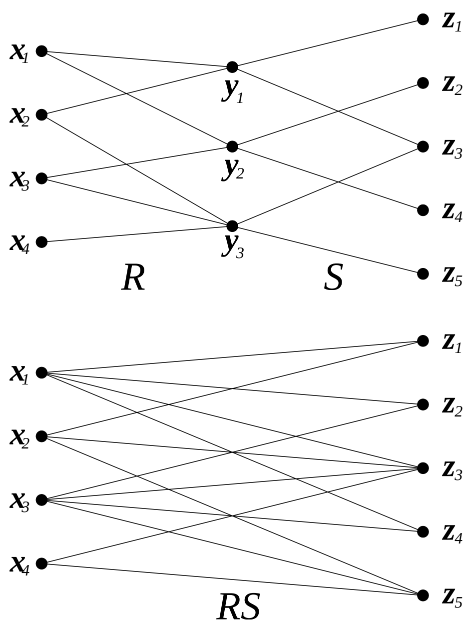
$$R^k = R^{k-1} \circ R, \quad k \geq 2.$$

Remark. Given relations $R \subseteq X \times Y$ and $S \subseteq Y \times Z$, the composition $S \circ R$ of R and S is backward. However, some people use the notation $R \circ S$ instead of our notation $S \circ R$. But this usage is inconsistent with the composition of functions. To avoid confusion and for aesthetic reason, we write $S \circ R$ as

$$RS = \{(x, z) \in X \times Z : \exists y \in Y,\ xRy,\ ySz\}.$$

Example 3.1. Let $R \subseteq X \times Y$, $S \subseteq Y \times Z$, where

$$X = \{x_1, x_2, x_3, x_4\},\ Y = \{y_1, y_2, y_3\},\ Z = \{z_1, z_2, z_3, z_4, x_5\}.$$



Example 3.2. For the brother-sister relation, sister-brother relation, brother relation, and sister relation on $A = \{a, b, c, d, e\}$, we have

$$R_{bs}R_{sb} = R_b,\ \ R_{sb}R_{bs} = R_s,\ \ R_{bs}R_s = R_{bs},$$
$$R_{bs}R_{bs} = \varnothing,\quad R_bR_b = R_b,\quad R_bR_s = \varnothing.$$

Let X_1, X_2, …, X_n, X_{n+1} be nonempty sets. Given relations

$$R_i \subseteq X_i \times X_{i+1}, \quad 1 \leq i \leq n.$$

We define a relation $R_1R_2\cdots R_n \subseteq X_1 \times X_{n+1}$ from X_1 to X_{n+1} by

$$xR_1R_2\cdots R_n y,$$

if and only if there exists a sequence $x_1, x_2, \ldots, x_n, x_{n+1}$ with $x_1 = x$, $x_{n+1} = y$ such that

$$x_1R_1x_2, \quad x_2R_2x_3, \quad \ldots, \quad x_nR_nx_{n+1}.$$

Theorem 3.2. *Given relations*

$$R_1 \subseteq X_1 \times X_2, \quad R_2 \subseteq X_2 \times X_3, \quad R_3 \subseteq X_3 \times X_4.$$

We have

$$R_1R_2R_3 = R_1(R_2R_3) = (R_1R_2)R_3.$$

as relations from X_1 to X_4.

Proof. For $x \in X_1$, $y \in X_4$, we have

$$\begin{aligned} xR_1(R_2R_3)y &\Leftrightarrow \exists x_2 \in X_2,\ xR_1x_2,\ x_2R_2R_3y \\ &\Leftrightarrow \exists x_2 \in X_2,\ xR_1x_2; \\ &\quad\ \exists x_3 \in X_3,\ x_2R_2x_3,\ x_3R_3y \\ &\Leftrightarrow \exists x_2 \in X_2,\ x_3 \in X_3, \\ &\quad\ xR_1x_2,\ x_2R_2x_3,\ x_3R_3y \\ &\Leftrightarrow xR_1R_2R_3y. \end{aligned}$$

Similarly, $x(R_1R_2)R_3y \Leftrightarrow xR_1R_2R_3y$. $\square$

Proposition 3.3. *Let $R_i \subseteq X \times Y$ be relations, $i = 1, 2$.*

(a) If $R \subseteq W \times X$, then $R(R_1 \cup R_2) = RR_1 \cup RR_2$.

(b) If $S \subseteq Y \times Z$, then $(R_1 \cup R_2)S = R_1S \cup R_2S$.

Proof. (a) For each $wR(R_1 \cup R_2)y$, $\exists x \in X$ such that wRx and $x(R_1 \cup R_2)y$. Then xR_1y or xR_2y. Thus wRR_1y or wRR_2y. Namely, $w(RR_1 \cup RR_2)y$.

Conversely, for each $(w, y) \in RR_1 \cup RR_2$, we have either $(w, y) \in RR_1$ or $(w, y) \in RR_2$. Then there exist $x_1, x_2 \in X$ such that either $(w, x_1) \in R$, $(x_1, y) \in R_1 \subseteq R_1 \cup R_2$ or $(w, x_2) \in R$, $(x_2, y) \in R_2 \subseteq R_1 \cup R_2$. This means that there exists $x \in X$ such that $(w, x) \in R$, $(x, y) \in R_1 \cup R_2$. Thus $(w, y) \in R(R_1 \cup R_2)$.

The proof for (b) is similar. $\square$

Exercise 1. Let $R_i \subseteq X \times Y$ be relations, $i = 1, 2, \ldots$.

(a) If $R \subseteq W \times X$, then $R\left(\bigcup_{i=1}^{\infty} R_i\right) = \bigcup_{i=1}^{\infty} RR_i$.

(b) If $S \subseteq Y \times Z$, then $\left(\bigcup_{i=1}^{\infty} R_i\right)S = \bigcup_{i=1}^{\infty} R_iS$.

For the convenience of representing composition of relations, we introduce the **Boolean operations** $\wedge$ and $\vee$ on real numbers. For $a, b \in \mathbb{R}$, define

$$a \wedge b = \min\{a, b\}, \quad a \vee b = \max\{a, b\}.$$

Exercise 2. For $a, b, c \in \mathbb{R}$,

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Proof. We only prove the first formula. The second one is similar.

Case 1: $b \leq c$. If $a \geq c$, then the left side is $a \wedge (b \vee c) = a \wedge c = c$. The right side is $(a \wedge b) \vee (a \wedge c) = b \vee c = c$. If $b \leq a \leq c$, then the left side is $a \wedge (b \vee c) = a \wedge c = a$. The right side is $(a \wedge b) \vee (a \wedge c) = b \vee a = a$. If $a \leq b \leq c$, then the left side is $a \wedge (b \vee c) = a \wedge c = a$. The right side is $(a \wedge b) \vee (a \wedge c) = a \vee a = a$.

Case 2: $b \geq c$. If $a \leq c$, then $a \wedge (b \vee c) = a \wedge c = a$ and $(a \wedge b) \vee (a \wedge c) = a \vee a = a$. If $b \geq a \geq c$, then $a \wedge (b \vee c) = a \wedge c = a$ and $(a \wedge b) \vee (a \wedge c) = a \vee c = a$. If $a \geq b$, then $a \wedge (b \vee c) = a \wedge b = b$ and $(a \wedge b) \vee (a \wedge c) = b \vee c = b$. $\square$

Sometimes it is more convenient to write the Boolean operations as

$$a \odot b = \min\{a, b\}, \quad a \oplus b = \max\{a, b\}.$$

For real numbers $a_1, a_2, \ldots, a_n$, we define

$$\bigvee_{i=1}^{n} a_i = \bigoplus_{i=1}^{n} a_i = \max\{a_1, a_2, \ldots, a_n\}.$$

For an $m \times n$ matrix $A = [a_{ij}]$ and an $n \times p$ matrix $B = [b_{jk}]$, the **Boolean multiplication** of A and B is an $m \times p$ matrix $A * B = [c_{ik}]$, whose (i, k)-entry is defined by

$$c_{ik} = \bigvee_{j=1}^{n} (a_{ij} \wedge b_{jk}) = \bigoplus_{j=1}^{n} (a_{ij} \odot b_{jk}).$$

Theorem 3.4. *Let $R \subseteq X \times Y$, $S \subseteq Y \times Z$ be relations, where*

$$X = \{x_1, \dots, x_m\}, \quad Y = \{y_1, \dots, y_n\}, \quad Z = \{z_1, \dots, z_p\}.$$

Let M_R, M_S, M_{RS} be matrices of R, S, RS respectively. Then

$$M_{RS} = M_R * M_S.$$

Proof. We write $M_R = [a_{ij}]$, $M_S = [b_{jk}]$, and

$$M_R * M_S = [c_{ik}], \quad M_{RS} = [d_{ik}].$$

It suffices to show that $c_{ik} = d_{ik}$ for any (i,k)-entry.

Case I: $c_{ik} = 1$.

Since $c_{ik} = \bigvee_{j=1}^{n}(a_{ij} \wedge b_{jk}) = 1$, there exists j_0 such that $a_{ij_0} \wedge b_{j_0k} = 1$. Then $a_{ij_0} = b_{j_0k} = 1$. In other words, $x_i R y_{j_0}$ and $y_{j_0} S z_k$. Thus $x_i RS z_k$ by definition of composition. Therefore $d_{ik} = 1$ by definition of Boolean matrix of RS.

Case II: $c_{ik} = 0$.

Since $c_{ik} = \bigvee_{j=1}^{n}(a_{ij} \wedge b_{jk}) = 0$, we have $a_{ij} \wedge b_{jk} = 0$ for all j. Then there is no j such that $a_{ij} = 1$ and $b_{jk} = 1$. In other words, there is no $y_j \in Y$ such that both $x_i R y_j$ and $y_j S z_k$. Thus x_i is not related to z_k by definition of RS. Therefore $d_{ik} = 0$. $\square$

4 Special Relations

We are interested in some special relations satisfying certain properties. For instance, the "less than" relation on the set of real numbers satisfies the so-called transitive property: if $a < b$ and $b < c$, then $a < c$.

Definition 4.1. A binary relation R on a set X is said to be

(a) **reflexive** if xRx for all x in X;

(b) **symmetric** if xRy implies yRx;

(c) **transitive** if xRy and yRz imply xRz.

A relation R is called an **equivalence relation** if it is reflexive, symmetric, and transitive. And in this case, if xRy, we say that x and y are **equivalent**.

The relation $I_X = \{(x, x) : x \in X\}$ is called the **identity relation**. The relation X^2 is called the **complete relation**.

Example 4.1. Many family relations are binary relations on the set of human beings.

(a) The strict brother relation R_b: $xR_by \Leftrightarrow x$ and y are both males and have the same parents. (symmetric and transitive)

(b) The strict sister relation R_s: $xR_sy \Leftrightarrow x$ and y are both females and have the same parents. (symmetric and transitive)

(c) The strict brother-sister relation R_{bs}: $xR_{bs}y \Leftrightarrow x$ is male, y is female, x and y have the same parents.

(d) The strict sister-brother relation R_{sb}: $xR_{sb} \Leftrightarrow x$ is female, y is male, and x and y have the same parents.

(e) The generalized brother relation R'_b: $xR'_by \Leftrightarrow x$ and y are both males and have the same father or the same mother. (symmetric, not transitive)

(f) The generalized sister relation R'_s: $xR'_sy \Leftrightarrow x$ and y are both females and have the same father or the same mother. (symmetric, not transitive)

(g) The relation R: $xRy \Leftrightarrow x$ and y have the same parents. (reflexive, symmetric, and transitive; equivalence relation)

(h) The relation R': $xR'y \Leftrightarrow x$ and y have the same father or the same mother. (reflexive and symmetric)

Example 4.2. (a) The less than relation $<$ on the set of real numbers is a transitive relation.

(b) The less than or equal to relation $\leq$ on the set of real numbers is a reflexive and transitive relation.

(c) The divisibility relation on the set of positive integers is a reflexive and transitive relation.

(d) Given a positive integer n. The **congruence modulo** n is a relation $\equiv_n$ on $\mathbb{Z}$ defined by

$$a \equiv_n b \Leftrightarrow b - a \text{ is a multiple of } n.$$

The standard notation for $a \equiv_n b$ is $a \equiv b \bmod n$. The relation $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.

Theorem 4.2. *Let R be a relation on a set X with matrix M_R. Then*

(a) R is reflexive $\Leftrightarrow I \subseteq R \Leftrightarrow$ all diagonal entries of M_R are 1.

(b) R is symmetric $\Leftrightarrow R = R^{-1} \Leftrightarrow M_R$ is a symmetric matrix.

(c) *R is transitive $\Leftrightarrow R^2 \subseteq R \Leftrightarrow M_R^2 \leq M_R$.*

Proof. (a) and (b) are trivial.

(c) "R is transitive $\Rightarrow R^2 \subseteq R$."

For any $(x, y) \in R^2$, there exists $z \in X$ such that $(x, z) \in R$, $(z, y) \in R$. Since R is transitive, then $(x, y) \in R$. Thus $R^2 \subseteq R$.

"$R^2 \subseteq R \Rightarrow R$ is transitive."

For $(x, z) \in R$ and $(z, y) \in R$, we have $(x, y) \in R^2 \subset R$. Then $(x, y) \in R$. Thus R is transitive.

Note that for any relations R and S on X, we have

$$R \subseteq S \;\Leftrightarrow\; M_R \leq M_S.$$

Since M_R is the matrix of R, then $M_R^2 = M_R M_R = M_{RR} = M_{R^2}$ is the matrix of R^2. Thus $R^2 \subseteq R \Leftrightarrow M_R^2 \leq M_R$. □

5 Equivalence Relations and Partitions

The most important binary relations are equivalence relations. We will see that an equivalence relation on a set X will partition X into disjoint equivalence classes.

Example 5.1. Consider the congruence relation $\equiv_3$ on $\mathbb{Z}$. For each $a \in \mathbb{Z}$, define

$$[a] = \{b \in \mathbb{Z} : a \equiv_3 b\} = \{b \in \mathbb{Z} : a \equiv b \bmod 3\}.$$

It is clear that $\mathbb{Z}$ is partitioned into three disjoint subsets

$$\begin{array}{rcl} [0] &=& \{0, \pm 3, \pm 6, \pm 9, \ldots\} &=& \{3k : k \in \mathbb{Z}\}, \\ [1] &=& \{1, 1 \pm 3, 1 \pm 6, 1 \pm 9, \ldots\} &=& \{3k+1 : k \in \mathbb{Z}\}, \\ [2] &=& \{2, 2 \pm 3, 2 \pm 6, 2 \pm 9, \ldots\} &=& \{3k+2 : k \in \mathbb{Z}\}. \end{array}$$

Moreover, for all $k \in \mathbb{Z}$,

$$[0] = [3k], \quad [1] = [3k+1], \quad [2] = [3k+2].$$

Theorem 5.1. *Let $\sim$ be an equivalence relation on a set X. For each x of X, let $[x]$ denote the set of members equivalent to x, i.e.,*

$$[x] := \{y \in X \ : \ x \sim y\},$$

called the **equivalence class** *of x under $\sim$. Then*

(a) *$x \in [x]$ for any $x \in X$,*

(b) *$[x] = [y]$ if $x \sim y$,*

(c) *$[x] \cap [y] = \varnothing$ if $x \not\sim y$,*

(d) *$X = \bigcup_{x \in X} [x]$.*

The member x is called a **representative** *of the equivalence class $[x]$. The set of all equivalence classes*

$$X/\!\sim : \{[x] : x \in X\}$$

is called the **quotient set** *of X under the equivalence relation $\sim$ or modulo $\sim$.*

Proof. (a) It is trivial because $\sim$ is reflexive.

(b) For any $z \in [x]$, we have $x \sim z$ by definition of $[x]$. Since $x \sim y$, we have $y \sim x$ by the symmetric property of $\sim$. Then $y \sim x$ and $x \sim z$ imply that $y \sim z$ by transitivity of $\sim$. Thus $z \in [y]$ by definition of $[y]$; that is, $[x] \subset [y]$. Since $\sim$ is symmetric, we have $[y] \subset [x]$. Therefore $[x] = [y]$.

(c) Suppose $[x] \cap [y]$ is not empty, say $z \in [x] \cap [y]$. Then $x \sim z$ and $y \sim z$. By symmetry of $\sim$, we have $z \sim y$. Thus $x \sim y$ by transitivity of $\sim$, a contradiction.

(d) This is obvious because $x \in [x]$ for any $x \in X$. $\square$

Definition 5.2. A **partition** of a nonempty set X is a collection

$$\Pi = \{A_j : j \in J\}$$

of subsets of X such that

(a) $A_i \neq \varnothing$ for all i;

(b) $A_i \cap A_j = \varnothing$ if $i \neq j$;

(c) $X = \bigcup_{j \in J} A_j$.

Each subset A_j is called a **block** of the partition Π.

Theorem 5.3. *Let* Π *be a partition of a set* X*. Let* R_Π *denote the relation on* X *defined by*

$$xR_\Pi y \Leftrightarrow \exists \text{ a block } A_j \in \Pi \text{ such that } x, y \in A_j.$$

Then R_Π *is an equivalence relation on* X*, called the* **equivalence relation induced by** Π.

Proof. (a) For each $x \in X$, there exits one A_j such that $x \in A_j$. Then by definition of R_Π, $xR_\Pi x$. Hence R_Π is reflexive.

(b) If $xR_\Pi y$, then there is one A_j such that $x, y \in A_j$. By definition of R_Π, $yR_\Pi x$. Thus R_Π is symmetric.

(c) If $xR_\Pi y$ and $yR_\Pi z$, then there exist A_i and A_j such that $x, y \in A_i$ and $y, z \in A_j$. Since $y \in A_i \cap A_j$ and Π is a partition, it forces $A_i = A_j$. Thus $xR_\Pi z$. Therefore R_Π is transitive. □

Given an equivalence relation R on a set X. The collection

$$\Pi_R = \{[x] \ : \ x \in X\}$$

of equivalence classes of R is a partition of X, called the **quotient set** of X modulo R. Let $\boldsymbol{E}(X)$ denote the set of all equivalence relations on X and $\boldsymbol{\Pi}(X)$ the set of all partitions of X. Then we have two functions

$$f : \boldsymbol{E}(X) \to \boldsymbol{\Pi}(X), \quad f(R) = \Pi_R;$$

$$g : \boldsymbol{\Pi}(X) \to \boldsymbol{E}(X), \quad g(\Pi) = R_\Pi.$$

The functions f and g satisfy the following properties.

Theorem 5.4. *Let X be a nonempty set. Then for any equivalence relation R on X, and any partition Π of X, we have*

$$(g \circ f)(R) = R, \qquad (f \circ g)(\Pi) = \Pi.$$

In other words, f and g are inverse of each other.

Proof. Recall $(g \circ f)(R) = g(f(R))$, $(f \circ g)(\Pi) = f(g(\Pi))$. Then

$$\begin{array}{rcccl} x[g(\Pi_R)]y & \Leftrightarrow & \exists A \in \Pi_R \text{ s.t. } x, y \in A & \Leftrightarrow & xRy; \\ A \in f(R_\Pi) & \Leftrightarrow & \exists x \in X \text{ s.t. } A = R_\Pi(x) & \Leftrightarrow & A \in \Pi. \end{array}$$

Thus $g(f(R)) = R$ and $f(g(\Pi)) = \Pi$. $\square$

Example 5.2. *Let $\mathbb{Z}_+$ be the set of positive integers. Define a relation $\sim$ on $\mathbb{Z} \times \mathbb{Z}_+$ by*

$$(a, b) \sim (c, d) \;\Leftrightarrow\; ad = bc.$$

Is $\sim$ an equivalence relation? If Yes, what are the equivalence classes?

Let R be a relation on a set X. The **reflexive closure** of R is the smallest reflexive relation $r(R)$ on X that contains R; that is,

a) $R \subseteq r(R)$,

b) if R' is a reflexive relation on X and $R \subseteq R'$, then $r(R) \subseteq R'$.

The **symmetric closure** of R is the smallest symmetric relation $s(R)$ on X such that $R \subseteq s(R)$; that is,

a) $R \subseteq s(R)$,

b) if R' is a symmetric relation on X and $R \subseteq R'$, then $s(R) \subseteq R'$.

The **transitive closure** of R is the smallest transitive relation $t(R)$ on X such that $R \subseteq t(R)$; that is,

a) $R \subseteq t(R)$,

b) if R' is a transitive relation on X and $R \subseteq R'$, then $t(R) \subseteq R'$.

Obviously, the reflexive, symmetric, and transitive closures of R must be unique respectively.

Theorem 5.5. *Let R be a relation R on a set X. Then*

a) $r(R) = R \cup I$;

b) $s(R) = R \cup R^{-1}$;

c) $t(R) = \bigcup_{k=1}^{\infty} R^k$.

Proof. (a) and (b) are obvious.

(c) Note that $R \subseteq \bigcup_{k=1}^{\infty} R^k$ and

$$\left(\bigcup_{i=1}^{\infty} R^i\right)\left(\bigcup_{j=1}^{\infty} R^j\right) = \bigcup_{i,j=1}^{\infty} R^i R^j = \bigcup_{i,j=1}^{\infty} R^{i+j} = \bigcup_{k=2}^{\infty} R^k \subseteq \bigcup_{k=1}^{\infty} R^k.$$

This shows that $\bigcup_{k=1}^{\infty} R^k$ is a transitive relation, and $R \subseteq \bigcup_{k=1}^{\infty} R^k$. Since each transitive relation that contains R must contain R^k for all integers $k \geq 1$, we see that $\bigcup_{k=1}^{\infty} R^k$ is the transitive closure of R. $\square$

Example 5.3. Let $X = \{a, b, c, d, e, f, g\}$ and consider the relation

$$R = \{(a, b), (b, b), (b, c), (d, e), (e, f), (f, g)\}.$$

Then the reflexive closure of R is

$$\begin{aligned} r(R) \;=\; & \{(a, a), (a, b), (b, b), (b, c), (c, c), (d, d), \\ & (d, e), (e, e), (e, f), (f, f), (f, g), (g, g)\}. \end{aligned}$$

The symmetric closure is

$$\begin{aligned} s(R) \;=\; & \{((a, b), (b, a), (b, b), (b, c), (c, b), (d, e), \\ & (e, d), (e, f), (f, e), (f, g), (g, f)\}. \end{aligned}$$

The transitive closure is

$$\begin{aligned} t(R) \;=\; & \{(a, b), (a, c), (b, b), (b, c), (d, e), \\ & (d, f), (d, g), (e, f), (e, g), (f, g)\}. \end{aligned}$$

$$R^2 = \{(a, b), (a, c), (b, b), (b, c), (d, f), (e, g)\}$$

$$R^3 = \{(a, b), (a, c), (b, b), (b, c), (d, g)\},$$

$$R^k = \{(a, b), (a, c), (b, b), (b, c)\}, \quad k \geq 4.$$

Theorem 5.6. *Let R be a relation on a set X with $|X| = n \geq 2$. Then*

$$t(R) = R \cup R^2 \cup \cdots \cup R^{n-1}.$$

In particular, if R is reflexive, then $t(R) = R^{n-1}$.

Proof. It is enough to show that for all $k \geq n$,

$$R^k \subseteq \bigcup_{i=1}^{n-1} R^i.$$

This is equivalent to showing that $R^k \subseteq \bigcup_{i=1}^{k-1} R^i$ for all $k \geq n$.

Let $(x, y) \in R^k$. There exist elements $x_1, \ldots, x_{k-1} \in X$ such that

$$(x, x_1),\ (x_1, x_2),\ \ldots,\ (x_{k-1}, y) \in R.$$

Since $|X| = n \geq 2$ and $k \geq n$, the following sequence

$$x = x_0,\ x_1,\ x_2,\ \ldots,\ x_{k-1},\ x_k = y$$

has $k + 1$ terms, which is at least $n + 1$. Then two of them must be equal, say, $x_p = x_q$ with $p < q$. Thus $q - p \geq 1$ and

$$(x_0, x_1),\ \ldots,\ (x_{p-1}, x_p),\ (x_q, x_{q+1}),\ \ldots,\ (x_{k-1}, x_k) \in R.$$

Therefore

$$(x, y) = (x_0, x_k) \in R^{k-(q-p)} \subseteq \bigcup_{i=1}^{k-1} R^i.$$

That is

$$R^k \subseteq \bigcup_{i=1}^{k-1} R^i.$$

If R is reflexive, then $R^k \subseteq R^{k+1}$ for all $k \geq 1$. Hence

$$t(R) = R^{n-1}.$$

□

Proposition 5.7. *Let R be a relation on a set X. Then*

$$I \cup t(R \cup R^{-1})$$

is an equivalence relation. In particular, if R is reflexive and symmetric, then $t(R)$ is an equivalence relation.

Proof. Since $I \cup t(R \cup R^{-1})$ is reflexive and transitive, we only need to show that $I \cup t(R \cup R^{-1})$ is symmetric.

Let $(x, y) \in I \cup t(R \cup R^{-1})$. If $x = y$, then obviously

$$(y, x) \in I \cup t(R \cup R^{-1}).$$

If $x \neq y$, then $(x, y) \in t(R \cup R^{-1})$. Thus $(x, y) \in (R \cup R^{-1})^k$ for some $k \geq 1$. Hence there is a sequence

$$x = x_0,\ x_1,\ \ldots,\ x_k = y$$

such that

$$(x_i, x_{i+1}) \in R \cup R^{-1}, \quad 0 \leq i \leq k - 1.$$

Since $R \cup R^{-1}$ is symmetric, we have

$$(x_{i+1}, x_i) \in R \cup R^{-1}, \quad 0 \leq i \leq k - 1.$$

This means that $(y, x) \in (R \cup R^{-1})^k$. Hence $(y, x) \in I \cup t(R \cup R^{-1})$. Therefore $I \cup t(R \cup R^{-1})$ is symmetric.

In particular, if R is reflexive and symmetric, then obviously

$$I \cup t(R \cup R^{-1}) = t(R).$$

This means that $t(R)$ is reflexive and symmetric. Since $t(R)$ is automatically transitive, so $t(R)$ is an equivalence relation. □

Let R be a relation on a set X. The **reachability relation** of R is a relation R^* on X defined by

$$xR^*y \Leftrightarrow x = y \quad \text{or} \quad \exists \text{ finite } x_1, x_2, \ldots, x_k$$

such that

$$(x, x_1),\ (x_1, x_2),\ \ldots,\ (x_k, y) \in R.$$

That is, $R^* = I \cup t(R)$.

Theorem 5.8. *Let R be a relation on a set X. Let M and M^* be the Boolean matrices of R and R^* respectively. If $|X| = n$, then*

$$M^* = I \vee M \vee M^2 \vee \cdots \vee M^{n-1}.$$

Moreover, if R is reflexive, then

$$R^k \subset R^{k+1},\ k \geq 1;$$

$$M^* = M^{n-1}.$$

Proof. It follows from Theorem 5.6. □

6 Washall's Algorithm

Let R be a relation on $X = \{x_1, \ldots, x_n\}$. Let $y_0, y_1, \ldots, y_m$ be a path in R. The vertices $y_1, \ldots, y_{m-1}$ are called **interior vertices** of the path. For each k with $0 \leq k \leq n$, we define the Boolean matrix

$$W_k = [w_{ij}],$$

where $w_{ij} = 1$ if there is a path in R from x_i to x_j whose interior vertices are contained in

$$X_k := \{x_1, \ldots, x_k\},$$

otherwise $w_{ij} = 0$, where $X_0 = \varnothing$.

Since the interior vertices of any path in R is obviously contained in the whole set $X = X_n = \{x_1, \ldots, x_n\}$, the (i, j)-entry of W_n is equal to 1 if there is a path in R from x_i to x_j. Then W_n is the matrix of the transitive closure $t(R)$ of R, that is,

$$W_n = M_{t(R)}.$$

Clearly, $W_0 = M_R$. We have a sequence of Boolean matrices

$$M_R = W_0, \quad W_1, \quad W_2, \quad \ldots, \quad W_n.$$

The so-called **Warshall's algorithm** is to compute W_k from W_{k-1}, $k \geq 1$.

Let $W_{k-1} = [s_{ij}]$ and $W_k = [t_{ij}]$. If $t_{ij} = 1$, there must be a path

$$x_i = y_0,\ y_1,\ \ldots,\ y_m = x_j$$

from x_i to x_j whose interior vertices $y_1, \ldots, y_{m-1}$ are contained in $\{x_1, \ldots, x_k\}$. We may assume that $y_1, \ldots, y_{m-1}$ are distinct. If x_k is not an interior vertex of this path, that is, all interior vertices are contained in $\{x_1, \ldots, x_{k-1}\}$, then $s_{ij} = 1$. If x_k is an interior vertex of the path, say $x_k = y_p$, then there two sub-paths

$$x_i = y_0, \quad y_1, \quad \ldots, \quad y_p = x_k,$$
$$x_k = y_p, \quad y_{p+1}, \quad \ldots, \quad y_m = x_j$$

whose interior vertices $y_1, \ldots, y_{p-1}, y_{p+1}, \ldots, y_{m-1}$ are contained in $\{x_1, \ldots, x_{k-1}\}$ obviously. It follows that

$$s_{ik} = 1, \quad s_{kj} = 1.$$

We conclude that

$$t_{ij} = 1 \Leftrightarrow \begin{cases} s_{ij} = 1 & \text{or} \\ s_{ik} = 1, \quad s_{kj} = 1 & \text{for some} \quad k. \end{cases}$$

Theorem 6.1 (Warshall's Algorithm for Transitive Closure)**.** *Working on the Boolean matrix W_{k-1} to produce W_k.*

(a) *If the (i, j)-entry of W_{k-1} is 1, so is the entry in W_k. Keep 1 there.*

(b) *If the (i, j)-entry of W_{k-1} is 0, then check the entries of W_{k-1} at (i, k) and (k, j). If both entries are 1, then change the (i, j)-entry in W_{k-1} to 1. Otherwise, keep 0 there.*

Example 6.1. Consider the relation R on $A = \{1, 2, 3, 4, 5\}$ given by the Boolean matrix

$$M_R = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

By Warshall's algorithm, we have

$$W_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \Rightarrow W_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & (1) \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} (3,1),(1,5)$$

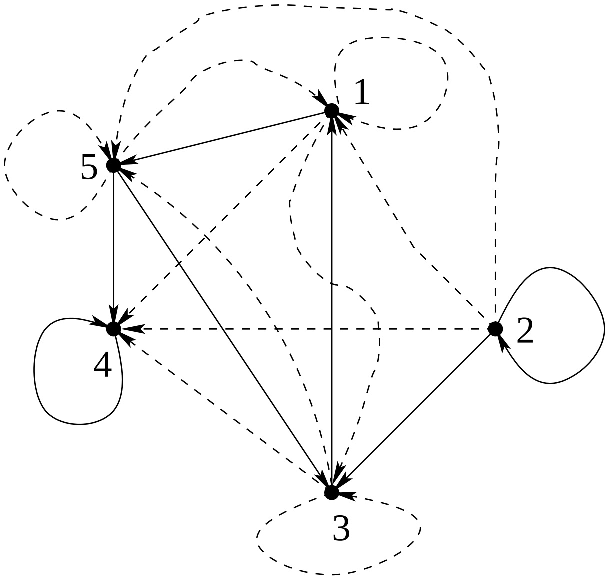
$$\Rightarrow W_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix} \text{(no change)}$$

$$\Rightarrow W_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ (1) & 1 & 1 & 0 & (1) \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ (1) & 0 & 1 & 1 & (1) \end{bmatrix} \begin{matrix} (2,3),(3,1) \\ (2,3),(3,5) \\ (5,3),(3,1) \\ (5,3),(3,5) \end{matrix}$$

$$\Rightarrow W_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix} \text{(no change)}$$

$$\Rightarrow W_5 = \begin{bmatrix} (1) & 0 & (1) & (1) & 1 \\ 1 & 1 & 1 & (1) & 1 \\ 1 & 0 & (1) & (1) & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{matrix} (1,5),(5,1) \\ (1,5),(5,3) \\ (1,5),(5,4) \\ (2,5),(5,4) \\ (3,5),(5,3) \\ (3,5),(5,4) \end{matrix}.$$

The binary relation for the Boolean matrix W_5 is the transitive closure of R.



Definition 6.2. A binary relation R on a set X is called

a) **asymmetric** if xRy implies $y\bar{R}x$;

b) **antisymmetric** if xRy and yRx imply $x = y$.

7 Modular Integers

For an equivalence relation $\sim$ on a set X, the set of equivalence classes is usually denoted by $X/\sim$, called the **quotient set** of X modulo $\sim$. Given a positive integer $n \geq 2$. The **relation modulo** n, denoted $\equiv_n$, is a binary relation on $\mathbb{Z}$, defined as $a \equiv_n b$ if $b - a = kn$ for an integer $k \in \mathbb{Z}$. Traditionally, $a \equiv_n b$ is written as $a \equiv b \pmod{n}$. We denote the quotient set $\mathbb{Z}/\equiv_n$ by

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

There addition and multiplication on $\mathbb{Z}_n$, defined as

$$[a] + [b] = [a+b], \quad [a][b] = [ab].$$

The two operations are well defined since

$$[a+kn] + [b+ln] = [(a+b) + (k+l)n]] = [a+b],$$

$$[a+kn][b+ln] = [[(a+kn)(b+ln)] = [ab+(al+bk+kl)n]] = [ab].$$

A modular integer $[a]$ is said to be **invertible** if there exists an modular integer $[b]$ such that $[a][b] = [1]$. If so, $[b]$ is called the **inverse** of $[a]$, written

$$[b] = [a]^{-1}.$$

If an inverse exists, it must be unique. If $[b]$ is an inverse of $[a]$, then $[a]$ is an inverse of $[b]$.

A modular integer $[a]$ is said to be **invertible** if there exists an modular integer $[c]$ such that $[a][b] = [1]$. If so, $[b]$ is called the **inverse** of $[a]$, written $[b] = [a]^{-1}$. If $[a_1], [a_2]$ are invertible, then $[a_1][a_2] = [a_1 a_2]$ is invertible. Let $[b_1], [b_2]$ be inverses of $[a_1], [a_2]$ respectively. Then $[b_1 b_2]$ is the inverse of $[a_1 a_2]$. In fact, $[a_1 a_2][b_1 b_2] = [a_1][a_2][b_2][b_1] = [a_1][1][b_1] = [a_1][b_1] = [1]$.

Example 7.1. What modular integers $[a]$ are invertible in $\mathbb{Z}_n$?

When $[a]$ has an inverse $[b]$, we have $[a][b] = 1$, i.e., $[ab] = [1]$. This means that ab and 1 are different by a multiple of n, say, $ab + kn = 1$ for an integer k. Let $d = \gcd(a, n)$. Then $d \mid (ab + kn)$, since $d \mid a$ and $d \mid n$. Thus $d \mid 1$. It forces $d = 1$. So $\gcd(a, n) = 1$.

If $\gcd(a, n) = 1$, by Euclidean Algorithm, there are integers x, y such that $ax + ny = 1$. Then $[ax + ny] = [ax] = [1]$, i.e., $[a][x] = [1]$. So $[x]$ is the inverse of $[a]$.

Example 7.2. Given an integer a. Consider the function

$$f_a : \mathbb{Z}_n \to \mathbb{Z}_n, \quad f_a([x]) = [ax].$$

Find a condition for a so that f_a is an invertible function.

Example 7.3. Is the function $f_{45} : \mathbb{Z}_{119} \to \mathbb{Z}_{119}$ by $f_{45}([x]) = [45x]$ invertible? If yes, find its inverse function.

We need to find $\gcd(119, 45)$ first. Applying the Division Algorithm,

$$\begin{aligned}
119 &= 2 \cdot 45 + 29 \\
45 &= 29 + 16 \\
29 &= 16 + 13 \\
16 &= 13 + 3 \\
13 &= 4 \cdot 3 + 1
\end{aligned}$$

So $\gcd(119, 45) = 1$. The function f_{45} is invertible. To find the inverse of f_{45}, we apply the Euclidean Algorithm:

$$\begin{aligned} 1 &= 13 - 4 \cdot 3 = 13 - 4(16 - 13) \\ &= 5 \cdot 13 - 4 \cdot 16 = 5(29 - 16) - 4 \cdot 16 \\ &= 5 \cdot 29 - 9 \cdot 16 = 5 \cdot 29 - 9(45 - 29) \\ &= 14 \cdot 29 - 9 \cdot 45 = 14(119 - 2 \cdot 45) - 9 \cdot 45 \\ &= 14 \cdot 119 + (\underline{-37}) \cdot 45 \end{aligned}$$

The inverse of f_{45} is f_{-37}, i.e., f_{82}.

Theorem 7.1 (Fermat's Little Theorem)**.** *Let p be a prime number and a an integer. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. The function $f_a : \mathbb{Z}_p \to \mathbb{Z}_p$ is invertible, since $\gcd(a, p) = 1$. So f_a is a bijection and $f_a(\mathbb{Z}_p) = \mathbb{Z}_p$. Since $f_a([0]) = [0]$, we must have

$$f_a(\mathbb{Z}_p - \{[0]\}) = \{[a], [2a], \ldots, [(p-1)a]\} = \{[1], \ldots, [p-1]\}.$$

Thus

$$\prod_{k=1}^{p-1}[ka] = \prod_{k=1}^{p-1}[k], \quad \text{i.e.,} \quad [a]^{p-1}\prod_{k=1}^{p-1}[k] = \prod_{k=1}^{p-1}[k][a] = \prod_{k=1}^{p-1}[k].$$

Since the product of invertible elements are still invertible, so $\prod_{k=1}^{p-1}[k]$ is invertible. Thus $[a^{p-1}] = [a]^{p-1} = [1]$. This means that $a^{p-1} \equiv 1 \pmod{p}$. $\square$

Let $\varphi(n)$ denote the number of positive integers coprime to n, i.e.,

$$\varphi(n) = |\{a \in [n] : \gcd(a, n) = 1\}.$$

For example, $p = 5$, $a = 6$ and $a \nmid 5$. Then $6^4 = 1296 = 1 \pmod{5}$.

Theorem 7.2 (Euler's Theorem)**.** *For integer $n \geq 2$ and integer a such that* $\gcd(a, n) = 1$,

$$a^{\varphi(n)} = 1 \pmod{n}.$$

Proof. Let $\mathbb{S}$ denote the set of invertible elements of $\mathbb{Z}_n$. Then $|\mathbb{S}| = \varphi(n)$. The elements $[a][s]$, $[s] \in \mathbb{S}$, are all distinct and invertible, i.e., $[a][s_1] \neq [a][s_2]$

for $[s_1], [s_2] \in S$ with $[s_1] \neq [s_2]$. In fact, $[a][s_1] = [a][s_2]$ implies $[s_1] = [s_2]$. Consider the product

$$[a]^{|\mathbb{S}|} \prod_{[s]\in\mathbb{S}} [s] = \prod_{[s]\in\mathbb{S}} [a][s] = \prod_{[s]\in\mathbb{S}} [s].$$

It follows that $[a]^{|\mathbb{S}|} = [1]$. $\square$

For example, $n = 12$, $a = 35$, $\gcd(35, 12) = 1$, and $\varphi(12) = \{1, 5, 7, 11\}$, $35^4 = 1500625 = 1 \pmod{12}$.

Problem Set 3

1. Let R be a binary relation from X to Y, $A, B \subseteq X$.

   (a) If $A \subseteq B$, then $R(A) \subseteq R(B)$.

   (b) $R(A \cup B) = R(A) \cup R(B)$.

   (c) $R(A \cap B) \subseteq R(A) \cap R(B)$.

   Proof. (a) For each $y \in R(A)$, there is an $x \in A$ such that $(x, y) \in R$. Clearly, $x \in B$, since $A \subseteq B$. Thus $y \in R(B)$. This means that $R(A) \subseteq R(B)$.

   (b) Since $R(A) \subseteq R(A \cup B)$, $R(B) \subseteq R(A \cup B)$, we have

   $$R(A) \cup R(B) \subseteq R(A \cup B).$$

   On the other hand, for each $y \in R(A \cup B)$, there is an $x \in A \cup B$ such that $(x, y) \in R$. Then either $x \in A$ or $x \in B$. Thus $y \in R(A)$ or $y \in R(B)$, i.e., $y \in R(A) \cup R(B)$. Therefore $R(A) \cup R(B) \supseteq R(A \cup B)$.

   (c) It follows from (a) that $R(A \cap B) \subseteq R(A)$ and $R(A \cap B) \subseteq R(B)$. Hence $R(A \cap B) \subseteq R(A \cap B)$. $\square$

2. Let R_1 and R_2 be relations from X to Y. If $R_1(x) = R_2(x)$ for all $x \in X$, then $R_1 = R_2$.

   Proof. For each $(x, y) \in R_1$, we have $y \in R_1(x)$. Since $R_1(x) = R_2(x)$, then $y \in R_2(x)$. Thus $(x, y) \in R_2$. Likewise, for each $(x, y) \in R_2$, we have $(x, y) \in R_2$. Hence $R_1 = R_2$. $\square$

3. Let $a, b, c \in \mathbb{R}$. Then

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

Proof. Note that the cases $b < c$ and $b > c$ are equivalent. There are three essential cases to be verified.

Case 1: $a < b < c$. We have

$$a \wedge (b \vee c) = a = (a \wedge b) \vee (a \wedge c),$$

$$a \vee (b \wedge c) = b = (a \vee b) \wedge (a \vee c).$$

Case 2: $b < a < c$. We have

$$a \wedge (b \vee c) = a = (a \wedge b) \vee (a \wedge c),$$

$$a \vee (b \wedge c) = a = (a \vee b) \wedge (a \vee c).$$

Case 3: $b < c < a$. We have

$$a \wedge (b \vee c) = c = (a \wedge b) \vee (a \wedge c),$$

$$a \vee (b \wedge c) = a = (a \vee b) \wedge (a \vee c).$$

$\square$

4. Let $R_i \subseteq X \times Y$ be a family of relations from X to Y, indexed by $i \in I$.

(a) If $R \subseteq W \times X$, then $R\left(\bigcup_{i \in I} R_i\right) = \bigcup_{i \in I} RR_i$;

(b) If $S \subseteq Y \times Z$, then $\left(\bigcup_{i \in I} R_i\right) S = \bigcup_{i \in I} R_i S$.

Proof. (a) By definition of composition of relations, $(w, y) \in R\left(\bigcup_{i \in I} R_i\right)$ is equivalent to that there exists an $x \in X$ such that $(w, x) \in R$ and $(x, y) \in \bigcup_{i \in I} R_i$. Notice that $(x, y) \in \bigcup_{i \in I} R_i$ is further equivalent to that there is an index $i_0 \in I$ such that $(x, y) \in R_{i_0}$. Thus $(w, y) \in R\left(\bigcup_{i \in I} R_i\right)$ is equivalent to that there exists an $i_0 \in I$ such that $(w, y) \in RR_i$, which means $(w, y) \in \bigcup_{i \in I} RR_i$ by definition of composition.

(b) $(x,z) \in \left(\bigcup_{i\in I} R_i\right) S \Leftrightarrow$ (by definition of composition) there exists $y \in Y$ such that $(x,y) \in \bigcup_{i\in I} R_i$ and $(y,z) \in S \Leftrightarrow$ (by definition of set union) there exists $i_0 \in I$ such that $(x,y) \in R_{i_0}$ and $(y,z) \in S \Leftrightarrow$ there exists $i_0 \in I$ such that $(w,y) \in RR_i \Leftrightarrow$ (by definition of composition) $(w,y) \in \bigcup_{i\in I} RR_i$. $\square$

5. Let R_i $(1 \le i \le 3)$ be relations on $A = \{a,b,c,d,e\}$ whose Boolean matrices are

$$M_1 = \begin{bmatrix} 0&1&1&0&1\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 0&1&1&0&1\\ 0&0&0&0&0 \end{bmatrix}, \; M_2 = \begin{bmatrix} 1&0&0&1&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ 1&0&0&1&0\\ 0&0&0&0&0 \end{bmatrix},$$

$$M_3 = \begin{bmatrix} 0&0&0&0&0\\ 0&1&1&0&1\\ 0&1&1&0&1\\ 0&0&0&0&0\\ 0&1&1&0&1 \end{bmatrix}.$$

(a) Draw the digraphs of the relations R_1, R_2, R_3.

(b) Find the Boolean matrices for the relations

$$R_1^{-1}, \quad R_2 \cup R_3, \quad R_1R_1, \quad R_1R_1^{-1}, \quad R_1^{-1}R_1;$$

and verify that

$$R_1R_1^{-1} = R_2, \quad R_1^{-1}R_1 = R_3.$$

(c) Verify that $R_2 \cup R_3$ is an equivalence relation and find the quotient set $A/(R_2 \cup R_3)$.

Solution:

$$M_{R_1^{-1}} = \begin{bmatrix} 0&0&0&0&0\\ 1&0&0&1&0\\ 1&0&0&1&0\\ 0&0&0&0&0\\ 1&0&0&1&0 \end{bmatrix}, \; M_{R_2\cup R_3} = \begin{bmatrix} 1&0&0&1&0\\ 0&1&1&0&1\\ 0&1&1&0&1\\ 1&0&0&1&0\\ 0&1&1&0&1 \end{bmatrix}, \; M_{R_1^2} = \begin{bmatrix} 0&0&0\\ 0&0&0\\ 0&0&0\\ 0&0&0\\ 0&0&0 \end{bmatrix}$$

$$M_{R_1R_1^{-1}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = M_2, \quad M_{R_1^{-1}R_1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} = M_3.$$

6. Let R be a relation on $\mathbb{Z}$ defined by aRb if $a+b$ is an even integer.

   (a) Show that R is an equivalence relation on $\mathbb{Z}$.

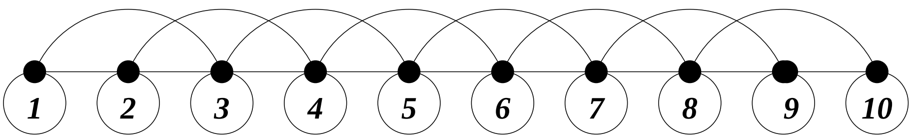
   (b) Find all equivalence classes of the relation R.

   Proof. (a) For each $a \in \mathbb{Z}$, $a + a = 2a$ is clearly even, so aRa, i.e., R is reflexive. If aRb, then $a+b$ is even, of course $b+a = a+b$ is even, so bRa, i.e., R is symmetric. If aRb and bRc, then $a+b$ and $b+c$ are even; thus $a+c = (a+b)+(b+c)-2b$ is even (sum of even numbers are even), so aRc, i.e., R is transitive. Therefore R is an equivalence relation.

   (b) Note that aRb if and only if both of a, b are odd or both are even. Thus there are exactly two equivalence classes: one class is the set of even integers, and the other class is the set of odd integers. The quotient set $\mathbb{Z}/R$ is the set $\mathbb{Z}_2$ of integers modulo 2. $\square$

7. Let $X = \{1, 2, \ldots, 10\}$ and let R be a relation on X such that aRb if and only if $|a-b| \le 2$. Determine whether R is an equivalence relation. Let M_R be the matrix of R. Compute M_R^8.

   Solution: The following is the graph of the relation.



   Then M_R^5 is a Boolean matrix all whose entries are 1. Thus M_R^8 is the same as M_R^5. $\square$

8. A relation R on a set X is called a **preference relation** if R is reflexive and transitive. Show that $R \cap R^{-1}$ is an equivalence relation.

Proof. Since $I \subseteq R$, we have $I = I^{-1} \subseteq R^{-1}$, so $I \subseteq R \cap R^{-1}$, i.e., $R \cap R^{-1}$ is reflexive.

If $x(R \cap R^{-1})y$, then xRy and $xR^{-1}y$; by definition of converse, $yR^{-1}x$ and yRx; thus $y(R \cap R^{-1})x$. This means that $R \cap R^{-1}$ is symmetric.

If $x(R \cap R^{-1})y$ and $y(R \cap R^{-1})z$, then xRy, yRz and yRx, zRy by converse; thus xRz and zRx by transitivity; therefore xRz and $xR^{-1}z$ by converse again; finally we have $x(R \cap R^{-1})z$. This means that $R \cap R^{-1}$ is transitive. □

9. Let n be a positive integer. The congruence relation $\sim$ of modulo n is an equivalence relation on $\mathbb{Z}$. Let $\mathbb{Z}_n$ denote the quotient set $\mathbb{Z}/\sim = \{[0], [1], \ldots, [n-1]\}$. Given an integer $a \in \mathbb{Z}$, we define a function

$$f_a : \mathbb{Z}_n \to \mathbb{Z}_n \quad \text{by} \quad f_a([x]) = [ax].$$

(a) Find the cardinality of the set $f_a(\mathbb{Z}_n)$.

(b) Find all integers a such that f_a is invertible.

Solution: (a) Let $d = \gcd(a, n)$, $a = kd$, $n = ld$. Fix an integer $x \in \mathbb{Z}$, we write $x = ql + r$ by division algorithm, where $0 \le r < l$. Then

$$ax = kd(ql + r) = kdql + kdr = kqn + ar \equiv ar \pmod{n}.$$

For two integers r_1, r_2 with $1 \le r_1 < r_2 < l$, we claim $ar_1 \not\equiv ar_2 \pmod{n}$. In fact, suppose $ar_1 \equiv ar_2 \pmod{n}$, then $n \mid a(r_2 - r_1)$; since $a = kd$ and $n = ld$, it is equivalent to $l \mid k(r_2 - r_1)$. Since $\gcd(k, l) = 1$, we have $l \mid (r_2 - r_1)$. Thus $r_1 = r_2$, which is a contradiction. Thus $|f_a(\mathbb{Z}_n)| = l = n/d$ and

$$f_a(\mathbb{Z}_n) = \{[ar] : r \in \mathbb{Z}, 0 \le r < l\}.$$

(b) Since $\mathbb{Z}_n$ is finite, then f_a is a bijection if and only if f_a is onto. However, f_a is onto if and only if $|f_a(\mathbb{Z}_n)| = n$, i.e., $\gcd(a, n) = 1$.

10. For a positive integer n, let $\phi(n)$ denote the number of positive integers $a \le n$ such that $\gcd(a, n) = 1$, called **Euler's function**. Let R be the relation on $X = \{1, 2, \ldots, n\}$ defined by aRb if $a \le b$, $b \mid n$, and $\gcd(a, b) = 1$.

(a) Find the cardinality $|R^{-1}(b)|$ for each $b \in X$.

(b) Show that

$$|R| = \sum_{a|n} \phi(a).$$

(c) Prove $|R| = n$ by showing that the function $f : R \to X$, defined by $f(a, b) = an/b$, is a bijection.

Solution: (a) For each $b \in X$, if $b \nmid n$, then $R^{-1}(b) = \varnothing$. If $b \mid n$, we have

$$|R^{-1}(b)| = |\{a \in X : a \leq b, \gcd(a, b) = 1\}| = \phi(b).$$

(b) It follows that

$$|R| = \sum_{b \in X} |R^{-1}(b)| = \sum_{b \geq 1,\, b|n} |R^{-1}(b)| = \sum_{b|n} \phi(b).$$

(c) The function f is clearly well-defined. We first to show that f is injective. For $(a_1, b_1), (a_2, b_2) \in R$, if $f(a_1, b_1) = f(a_2, b_2)$, i.e., $a_1 n/b_1 = a_2 n/b_2$, then $a_1/b_1 = a_2/b_2$, which is a rational number in reduced form, since $\gcd(a_1, b_1) = 1$ and $\gcd(a_2, b_2) = 1$; it follows that $(a_1, b_1) = (a_2, b_2)$. Thus f is injective. To see that f is surjective, for each $b \in X$, let $d = \gcd(b, n)$. Then $f(b/n, n/b) = (b/d)n/(n/d) = b$. This means that f is surjective. So f is a bijection. We have obtained the following formula

$$n = \sum_{b|n} \phi(b).$$