Math2343: 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 $R(A \cap B) \subseteq R(A \cap B)$. □

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 $R_1 = R_2$. □

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

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

   □

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) $(w, y) \in \bigcup_{i \in I} RR_i$. □

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

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

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

(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:

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

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

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 $\mathbb{Z}$.

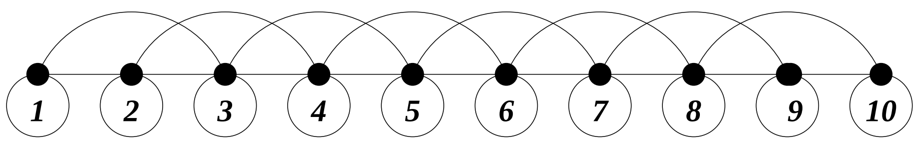
(b) Find all equivalence classes of the relation R.

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. □

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. □

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 $ar_1 = ar_2 \pmod{n}$, then $n \mid a(r_2 - r_1)$. It follows that $l \mid k(r_2 - r_1)$, since $a = kd$ and $n = ld$. Note that $\gcd(k, l) = 1$. It forces $l \mid (r_2 - r_1)$. 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

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

(b) It follows that

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

(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

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