Queen's University
School of Computing

CISC 203: Discrete Mathematics for Computing II
Module 2: Counting and Relations
Fall 2021

This module corresponds to the following sections from your textbook:

14. Relations
15. Equivalence Relations
16. Partitions

1 Relations

Definition 1 (Relation on a Set)**.** A **relation** is a set of two-element lists (i.e., ordered pairs). We say that R is a relation on a set A provided that $R \subseteq A \times A$.

Example 2. $R = \{(1,2),(2,3),(3,1)\}$ is a relation on the set $A = \{1,2,3\}$.

We say that an element x is related by the relation R to an element y if $(x,y) \in R$. We denote this by $x \; R \; y$; e.g., in the above example, we have $1 \; R \; 2$ and $3 \; R \; 1$.

If an element x is not related by the relation R to an element y, we denote this by $x \not R \, y$; e.g., in the example above, we have $1 \not R \, 3$ and $2 \not R \, 1$.

We say that R is a relation from a set A to a set B if $R \subseteq A \times B$.

Exercise

How many different relations on $A \times B$ are there?

Example 3. Let $A = \{1,2,3,4\}$ and $B = \{4,5,6,7\}$. Consider the following relations:

$$\begin{aligned}
R &= \{(1,1),(2,2),(3,3),(4,4)\} \\
S &= \{(1,2),(3,2)\}, \\
T &= \{(1,4),(1,5),(4,7)\}, \\
U &= \{(4,4),(5,2),(6,2),(7,3)\}, \\
V &= \{(1,7),(7,1)\}, \text{ and} \\
W &= E \times E, \text{where } E \text{ is the set of even integers.}
\end{aligned}$$

R is a relation on A; we call this the equality relation on A, because $R = \{(a,a) : a \in A\}$.

S is a relation on A. Note that a relation on A is not required to contain all elements of A.

T is a relation from A to B, and U is a relation from B to A.

V is a relation, but it is neither a relation from A to B nor a relation from B to A.

W is not a relation on A or B. However, note that we can use set operations on relations (since relations themselves are sets). So, $W \cap (A \times B)$ is a relation from A to B. Similarly, $W \cap (B \times A)$ is a relation from B to A.

Exercise

In the above example, modify A and B such that V would be, simultaneously, a relation on A, a relation on B, a relation from A to B, and a relation from B to A.

Definition 4 (Inverse relation)**.** Let R be a relation. The inverse relation of R, denoted R^{-1}, is defined as

$$R^{-1} = \{(x, y) : (y, x) \in R\}.$$

In other words, the inverse relation R^{-1} is formed by reversing the order of all the ordered pairs in R.

Example 5. Let $A = \{1, 2, 3, 4\}$ and $B = \{4, 5, 6, 7\}$. Consider the following relations:

$$R = \{(1, 4), (2, 5), (3, 6), (4, 7)\}, \text{ and}$$
$$S = \{(4, 1), (5, 2), (6, 3), (7, 4)\}.$$

We have $S = R^{-1}$. Observe also that:

- $R = S^{-1}$.
- R is a relation from A to B, and S is a relation from B to A.

Proposition 6. *Let R be a relation. Then $(R^{-1})^{-1} = R$.*

Proof. As already mentioned, since a relation is a set, we use Proof Template 5 (from p. 44 of your textbook):

To prove that two sets A and B are equal, we show that:
1. For $x \in A$, we also have $x \in B$.
2. For $x \in B$, we also have $x \in A$.

For $(x, y) \in (R^{-1})^{-1}$, we have: $(y, x) \in R^{-1}$ and then $(x, y) \in R$. So, we have $(x, y) \in (R^{-1})^{-1} \to (x, y) \in R$.

Similarly, for $(x, y) \in R$, we have: $(y, x) \in R^{-1}$ and then $(x, y) \in (R^{-1})^{-1}$. So, we have $(x, y) \in R \to (x, y) \in (R^{-1})^{-1}$.

We have shown that $(x, y) \in (R^{-1})^{-1} \iff (x, y) \in R$, and therefore $(R^{-1})^{-1} = R$. $\square$

We define a number of properties of a relation R on a set A depending on which ordered pairs belong to the relation.

Definition 7 (Properties of relations)**.** Let R be a relation defined on a set A.

- R is **reflexive** if, for all $a \in A$, $(a, a) \in R$.
- R is **irreflexive** if, for all $a \in A$, $(a, a) \notin R$.
- R is **symmetric** if, whenever $(a_1, a_2) \in R$, $(a_2, a_1) \in R$.
- R is **antisymmetric** if, whenever $(a_1, a_2) \in R$ and $(a_2, a_1) \in R$, $a_1 = a_2$.
- R is **transitive** if, whenever $(a_1, a_2) \in R$ and $(a_2, a_3) \in R$, $(a_1, a_3) \in R$.

Note that, despite their names, the properties of symmetry and antisymmetry are not mutually exclusive. A relation may be both symmetric and antisymmetric. However, if a relation is reflexive, it cannot be irreflexive, and vice-versa.

Example 8. Let R be the relation defined on $\mathbb{Z}$ by $x \; R \; y$ if $x \leq y$. Then, R is:

- Reflexive: For all $x \in \mathbb{Z}$ we have $x \leq x$.

- Not symmetric: It is not true that whenever $x \leq y$ we also have $y \leq x$; e.g., $3 \leq 5$ but $5 \not\leq 3$.
- Antisymmetric: $x \leq y$ and $y \leq x$ implies $x = y$.
- Transitive: $x \leq y$ and $y \leq z$ implies $x \leq z$.

Exercise

Repeat Example 8 for the the $=$ and $<$ relations on the integers. Check your work against Example 14.8 and 14.10 (p. 75) in the textbook.

Exercise

Prove that if R is symmetric, we have $R = R^{-1}$. Hint: Use Proof Template 5, as done in Example 6.

Definition 9 ($a \mid b$)**.** Let $a, b \in \mathbb{Z}$ and $a \neq 0$. If $b = ak$ for some integer k (i.e., if b is a multiple of a), we say that a divides b, and denote this as $a \mid b$.

Example 10. Let R be the relation defined on $\mathbb{N}$ by $x\ R\ y$ if $x \mid y$. Then, R is:

- Reflexive: For all $x \in \mathbb{N}$ we have $x \mid x$.
- Not symmetric: e.g., $3 \mid 15$ but $15 \nmid 3$.
- Antisymmetric: $x \mid y$ and $y \mid x$ implies $x = y$.
- Transitive: $x \mid y$ and $y \mid z$ implies $x \mid z$.

Note that if we define the relation R on $\mathbb{Z}$ instead of $\mathbb{N}$, it is not antisymmetric, since $3 \mid -3$ and $-3 \mid 3$, but $3 \neq -3$. This shows that (i) the properties of a relation depend on the set that it is restricted to, and (ii) a relation may be simultaneously not symmetric and not antisymmetric.

2 Equivalence Relations

Definition 11 (Equivalence Relation)**.** An **equivalence relation** is a relation on a set A that is reflexive, symmetric, and transitive. If R is an equivalence relation on A and $a_1\ R\ a_2$, then the elements $a_1 \in A$ and $a_2 \in A$ are said to be equivalent with respect to R.

Example 12. Let $R = \{(1,2),(2,1),(2,2),(2,3),(3,3)\}$ on the set $A = \{1,2,3\}$. R is:

- Not reflexive: For $1 \in A$, we have $1 \not R\ 1$.
- Not symmetric: We have $2\ R\ 3$ but $3 \not R\ 2$.
- Not transitive: We have $1\ R\ 2$ and $2\ R\ 3$, but $1 \not R\ 3$.

However, $S = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$ is an equivalence relation on A.
$T = \{(1,1),(1,2),(2,1),(2,2),(3,3)\}$ is also an equivalence relation on A.

Example 13. Let R be the relation has-the-same-size-as defined on all finite subsets of $\mathbb{Z}$; i.e., $A\ R\ B$ for any two finite sets of integers A and B if and only if $|A| = |B|$. R is:

- Reflexive: For all finite subsets $A \subset \mathbb{Z}$ we have $|A| = |A|$ and thus $A\ R\ A$.
- Symmetric: For any two finite subsets $A, B \subset \mathbb{Z}$ where $|A| = |B|$ and thus $A\ R\ B$, we also have $|B| = |A|$ and thus $B\ R\ A$.
- Transitive: For any three finite subsets $A, B, C \subset \mathbb{Z}$ where $|A| = |B|$ and thus $A\ R\ B$, and $|B| = |C|$ and thus $B\ R\ C$, we have $|A| = |C|$ and thus $A\ R\ C$.

Definition 14 (Congruence modulo n)**.** Let n be a positive integer and x and y be any two integers. If $n|(x-y)$, we say that x and y are congruent modulo n. This is denoted $x \equiv y \mod n$.

Example 15. We have $10 \equiv 4 \mod 3$, since $3 \mid (10-4)$. However, $7 \not\equiv 4 \mod 2$, since $2 \nmid (7-4)$.

Exercise

Which of the following are true:
(i) $3 \equiv 15 \mod 5$ (ii) $2 \equiv 10 \mod 3$ (iii) $3 \equiv -7 \mod 5$ (iv) $-1 \equiv 1 \mod 2$

Example 16. Let n be a positive integer and let R be the relation defined on $\mathbb{Z}$ by $x\ R\ y$ if $x \equiv y \mod n$. Then, "$\equiv \mod n$" is an equivalence relation, since we have:

- "$\equiv \mod n$" is Reflexive: Let x be an arbitrary integer. We have $n \mid (x-x)$, since $x - x = 0 = 0n$ (i.e., 0 is the multiple of n, or indeed any number) and thus $n \mid 0$. Therefore $x \equiv x \mod n$.
- "$\equiv \mod n$" is Symmetric: Let x and y be integers and suppose $x \equiv y \mod n$. This means that $n|(x-y)$. So there is an integer k such that $(x-y) = kn$, and therefore $(y-x) = (-k)n$. So, $n|(y-x)$. Therefore $y \equiv x \mod n$.
- "$\equiv \mod n$" is Transitive: Let x, y, and z be integers. Suppose $x \equiv y \mod n$ and $y \equiv z \mod n$. This means that $x - y = kn$ for some integer k and $y - z = ln$ for some integer l. So,

$$\begin{aligned} x - z &= kn + y - (y - ln) \\ &= kn + ln \\ &= (k+l)n \end{aligned}$$

  This means that $n|(x-z)$, so $x \equiv z \mod n$.

An equivalence relation on a set A partitions the set A into **equivalence classes**, which we define formally below.

Definition 17 (Equivalence class)**.** Let R be an equivalence relation on a set A and let $a \in A$. The equivalence class of a, denoted $[a]$, is the set of all elements of A related by R to a, i.e.,

$$[a] = \{x \in A : x\ R\ a\}.$$

In other words, the equivalence class of $a \in A$ is a subset of A where all elements in the subset are equivalent to a with respect to the given relation.

Example 18. For the equivalence relation "$\equiv \mod 3$" on $\mathbb{Z}$, the equivalence class $[0]$ is the set

$$[0] = \{x \in \mathbb{Z} : x\ R\ 0\}.$$

Thus, $[0]$ is the set of all elements $x \in \mathbb{Z}$ where $x \equiv 0 \mod 3$, and thus $3|(x-0)$. In other words, $[0]$ contains all multiples of 3. Similarly, $[1]$ is the set of all elements $x \in \mathbb{Z}$ where $x \equiv 1 \mod 3$, and thus $3|(x-1)$. In other words, $[1]$ contains all integers where division by 3 results in a remainder of 1. Similarly, $[2]$ contains all integers where division by 3 results in a remainder of 2. Finally, we have:

$$\begin{aligned} &[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ &[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\} \\ &[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\} \\ &[3] = [0] \\ &[4] = [1] \\ &[5] = [2] \\ &\ldots \end{aligned}$$

Exercise

For the equivalence relation congruence modulo 2, show that the set $[0]$ is the set of even numbers and $[1]$ is the set of odd numbers. Compare your work with Example 15.7 on p. 81 of your textbook.

Let n be a positive integer and let k be an integer where $0 \leq k < n$. In general, for the equivalence relation "$\equiv \mod n$" on $\mathbb{Z}$, the equivalence class $[k]$ is the set of all integers where division by n results in the remainder k.

Proposition 19. *Let R be an equivalence relation on a set A and let $a, b \in A$. If $[a] \cap [b] \neq \emptyset$, $[a] = [b]$.*

For the proof, see Proposition 15.12 on p. 82 of your textbook.

The above proposition tells us that if two equivalence classes $[a]$ and $[b]$ have at least one element in common, we must have $[a] = [b]$. If $[a] \neq [b]$, we must have $a \cap b = \emptyset$, i.e., $[a]$ and $[b]$ must be disjoint.

Exercise

Using the proposition above, prove that $[6] = [1]$ for the equivalence relation "$\equiv \mod 5$".

Corollary 20. *Let R be an equivalence relation on a set A. The equivalence classes of R are nonempty, pairwise disjoint subsets of A whose union is A.*

Example 21. For the equivalence relation "$\equiv \mod 3$" on $\mathbb{Z}$, the equivalence classes $[0]$, $[1]$, and $[2]$ are pairwise disjoint and we have $[0] \cup [1] \cup [2] = \mathbb{Z}$.

Example 22. Let R be the relation has-the-same-size-as defined on all finite subsets of $\mathbb{Z}$, given earlier in Example 13; i.e., $A \; R \; B$ for any two finite sets of integers A and B if and only if $|A| = |B|$. By definition, we have

$$[\emptyset] = \{A \subseteq \mathbb{Z} : |A| = 0\} = \{\emptyset\}$$

since $\emptyset$ is the only set with cardinality zero. Recall from Module 1 that $\{\emptyset\}$ is not an empty set.

For $a \in \mathbb{Z}$, we have

$$[\{a\}] = \{A \subseteq \mathbb{Z} : |A| = 1\} = \{\ \ldots, \{-3\}, \{-2\}, \{-1\}, \{0\}, \{1\}, \{2\}, \{3\}, \ldots\}$$

Similarly, the equivalence class $[\{203, 221\}]$ is the set of all finite subsets of $\mathbb{Z}$ with cardinality 2. It should be clear that this is disjoint from the equivalence class $[a]$ above.

Note that in this example, we have infinitely many pairwise-disjoint equivalence classes whose union is equal to the set of all the finite subsets of $\mathbb{Z}$.

3 Partitions

Definition 23 (Partition)**.** A **partition** $\mathcal{P}$ of a set A is a set of nonempty, pairwise disjoint sets (called **parts**) whose union is A.

Example 24. Let $A = \{1, 2, 3, 4, 5\}$ and let $\mathcal{P} = \big\{\{1, 2\}, \{3, 4, 5\}\big\}$, so $\mathcal{P}$ is a partition of A with two parts $\{1, 2\}$ and $\{3, 4, 5\}$. Observe that the parts are nonempty and pairwise disjoint, and that their union is A.

We show, by example, how an equivalence relation on a set A can be used to form a partition $\mathcal{P}$ of the set A.

Example 25. For the equivalence relation "$\equiv \mod 2$" on $\mathbb{Z}$, we have $\mathcal{P} = \{[0], [1]\}$, where

$$[0] \cup [1] = \mathbb{Z}.$$

Observe also that the equivalence classes $[0]$ and $[1]$ are parts of $\mathcal{P}$, and that $[0] \cap [1] = \emptyset$.

Similarly, for the equivalence relation "$\equiv \mod 3$" on $\mathbb{Z}$, we have $\mathcal{P} = \{[0], [1], [2]\}$, where

$$[0] \cup [1] \cup [2] = \mathbb{Z}.$$

Note that $[0]$, $[1]$, and $[2]$ are pairwise-disjoint.

Example 26. Let n be a positive integer. For the equivalence relation "$\equiv \mod n$" on $\mathbb{Z}$, we have the partition $\mathcal{P} = \{[0], [1], [2], \ldots [n-1]\}$, where we have the disjoint union

$$\bigcup_{k=0}^{n-1} [k] = \mathbb{Z}.$$

We learned that an when we have an equivalence relation on a set A, we can generate a partition $\mathcal{P}$ of A.

We now go in the opposite direction, and show by example that when we have a partition $\mathcal{P}$ of a set A, we can define the "is-in-the-same-part-as" equivalence relation on A, denoted $\stackrel{\mathcal{P}}{\equiv}$.

Example 27. Let $A = \{1, 2, 3, 4, 5, 6, 7\}$ and let $\mathcal{P} = \big\{\{1, 2, 4\}, \{3, 6\}, \{5, 7\}\big\}$, so $\mathcal{P}$ is a partition of A. We can now define an equivalence relation R on A as follows: $a \stackrel{\mathcal{P}}{\equiv} b$ (i.e., $a \mathrel{R} b$) if and only if both a and b are in the same part of the partition $\mathcal{P}$. So, we write $1 \stackrel{\mathcal{P}}{\equiv} 2$, $3 \stackrel{\mathcal{P}}{\equiv} 3$, and $5 \stackrel{\mathcal{P}}{\equiv} 7$. We also write $1 \stackrel{\mathcal{P}}{\not\equiv} 3$.

Exercise

The example above defines the relation $R = \{(1, 1), (2, 2), (4, 4), (1, 2), (2, 1), (1, 4), (4, 1), (2, 4), (4, 2), \ldots\}$. Fill in the $\ldots$ with the remaining ordered pairs in the relation.

Convince yourself that this relation is an equivalence relation and that the equivalence classes are the parts of $\mathcal{P}$.

In general, we have the following proposition.

Proposition 28. *Let A be a set and let $\mathcal{P}$ be a partition on A. The relation $\stackrel{\mathcal{P}}{\equiv}$ is an equivalence relation on A.*

See Proposition 16.3 (p. 86) in the textbook for the proof.

Finally, note the following two propositions.

Proposition 29. *Every equivalence class of the relation $\stackrel{\mathcal{P}}{\equiv}$ is a part of $\mathcal{P}$ and conversely every part of $\mathcal{P}$ is an equivalence class of the relation $\stackrel{\mathcal{P}}{\equiv}$.*

Theorem 30. *Let R be an equivalence relation on a finite set A. If all the equivalence classes of R have the same size, m, then the number of equivalence classes is $\frac{|A|}{m}$.*

We conclude this module with the following example, which uses Theorem 30 to solve a counting problem.

Example 31. Let us count the number of rearrangements of the word KAPPA. This is a list counting problem, but the difficulty arises from the fact that there are **indistinguishable elements** in the list (i.e., the letters that appear twice are indistinguishable from each other), so our answer is not simply 5! as would be the case for a word like DELTA.

We first distinguish the repeated letters from each other by subscripting them as follows:

$$\text{K A}_1 \text{ P}_1 \text{ P}_2 \text{ A}_2.$$

Let X be the set of all rearrangements of the list $(\text{K}, \text{A}_1, \text{P}_1, \text{P}_2, \text{A}_2)$. Let R be the relation defined on X by $x\ R\ y$ for $x, y \in X$ if and only if x and y represent the same spelling after the subscripts are removed. For example, we have

$$(\text{K}, \text{A}_1, \text{P}_1, \text{P}_2, \text{A}_2)\ R\ (\text{K}, \text{A}_1, \text{P}_4, \text{P}_3, \text{A}_2).$$

Note that:

1. R is an equivalence relation on X, since it is reflexive, symmetric, and transitive (you may convince yourself of this).
2. There are 5 elements in the list $(\text{K}, \text{A}_1, \text{P}_1, \text{P}_2, \text{A}_2)$, so there are $5! = 120$ rearrangements.
3. The number of lists in each equivalence class is equal to the number rearrangements of the subscripted letters that give the same spelling after the subscripts are removed. For example, the equivalence class

   $$[(\text{K}, \text{A}_1, \text{P}_1, \text{P}_2, \text{A}_2)] = \big\{(\text{K}, \text{A}_1, \text{P}_1, \text{P}_2, \text{A}_2), (\text{K}, \text{A}_2, \text{P}_1, \text{P}_2, \text{A}_1), (\text{K}, \text{A}_1, \text{P}_2, \text{P}_1, \text{A}_2), (\text{K}, \text{A}_2, \text{P}_2, \text{P}_1, \text{A}_1)\big\}.$$

   Indeed, each equivalence class of R contains 4 elements (i.e., they are all the same size), which means that we can use Theorem 30. We can show this mathematically, since there are 2! ways to rearrange A_1 and A_2, and 2! ways to rearrange P_1 and P_2, so by the Multiplication Principle we have $2! \times 2! = 4$ possible rearrangements.
4. By Theorem 30, the number of equivalence classes of R is $\frac{5!}{2! \cdot 2!} = \frac{120}{4} = 30$. Note that this is equal to the number of ways to rearrange the letters in KAPPA (i.e., without subscripts).

Exercise

Repeat the steps in the example above to determine the number of rearrangements of the word AARDVARK. Check your answer on p. 88 of the textbook.