4190.101
Discrete Mathematics

Chapter 9 Relations

Gunhee Kim

[Based on S. Srinivasa Rao's Lecture Notes]

Equivalence Relations

Section 9.5

Section Summary

- Equivalence Relations
- Equivalence Classes
- Equivalence Classes and Partitions

Equivalence Relations

- **Definition 1**: A relation on a set A is called an *equivalence relation* if it is reflexive, symmetric, and transitive.
- **Definition 2**: Two elements a and b that are related by an equivalence relation are called *equivalent.* The notation $a \sim b$ is often used to denote that a and b are equivalent elements with respect to a particular equivalence relation.

Strings

- **Example**: Suppose that R is the relation on the set of strings of English letters such that $a\ R\ b$ if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string x. Is R an equivalence relation?
- **Solution**: Show that all of the properties of an equivalence relation hold.
  - *Reflexivity*: Because $l(a) = l(a)$, it follows that $a\ R\ a$ for all strings a.
  - *Symmetry*: Suppose that $a\ R\ b$. Since $l(a) = l(b)$, $l(b) = l(a)$ also holds and $b\ R\ a$.
  - *Transitivity*: Suppose that a R b and $b\ R\ c$. Since $l(a) = l(b)$,and $l(b) = l(c)$, $l(a) = l(c)$ also holds and $a\ R\ c$.

Congruence Modulo *m*

- **Example**: Let m be an integer with $m>1$. Show that the relation
  $R = \{(a,b) \mid a \equiv b \pmod{m}\}$
  is an equivalence relation on the set of integers.
- **Solution**: Recall that $a \equiv b \pmod{m}$ if and only if m divides $a-b$.
  - *Reflexivity*: $a \equiv a \pmod{m}$ since $a - a = 0$ is divisible by m since $0 = 0 \cdot m$.
  - *Symmetry*: Suppose that $a \equiv b \pmod{m}$. Then $a - b$ is divisible by m, and so $a - b = km$, where k is an integer. It follows that $b - a = (-k) m$, so $b \equiv a \pmod{m}$.
  - *Transitivity*: Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then m divides both $a - b$ and $b - c$. Hence, there are integers k and l with $a - b = km$ and $b - c = lm$. We obtain by adding the equations:
    $$a - c = (a - b) + (b - c) = km + lm = (k + l)\, m.$$
    Therefore, $a \equiv c \pmod{m}$.

Divides

- **Example**: Show that the "divides" relation on the set of positive integers is not an equivalence relation.
- **Solution**: The properties of reflexivity, and transitivity do hold, but there relation is not transitive. Hence, "divides" is not an equivalence relation.
  - *Reflexivity*: $a \mid a$ for all a.
  - *Not Symmetric*: For example, $2 \mid 4$, but $4 \nmid 2$. Hence, the relation is not symmetric.
  - *Transitivity*: Suppose that a divides b and b divides c. Then there are positive integers k and l such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so a divides c. Therefore, the relation is transitive.

Equivalence Classes

- **Definition 3**: Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the *equivalence class* of a. The equivalence class of a with respect to R is denoted by $[a]_R$.
- Note that $[a]_R = \{s \mid (a,s) \in R\}$.
- When only one relation is under consideration, we can write $[a]$, without the subscript R, for this equivalence class.
- If $b \in [a]_R$, then b is called a representative of this equivalence class. Any element of a class can be a representative of the class.
- The equivalence classes of the relation congruence modulo m are called the *congruence classes modulo m*. The congruence class of an integer a modulo m is denoted by $[a]_m$, so $[a]_m = \{\ldots, a-2m, a-m, a, a+m, a+2m, \ldots\}$. For example,

  $[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$ $[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

  $[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$ $[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

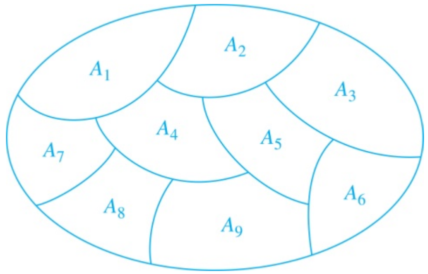
Equivalence Classes and Partitions

- **Theorem 1**: let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:
  (*i*) $a R b$
  (*ii*) $[a] = [b]$
  (*iii*) $[a] \cap [b] \neq \emptyset$
- **Proof:** We show that (*i*) implies (*ii*). Assume that $a R b$. Now suppose that $c \in [a]$. Then $a R c$. Because $a R b$ and R is symmetric, $b R a$. Because R is transitive and $b R a$ and $a R c$, it follows that $b R c$. Hence, $c \in [b]$. Therefore, $[a] \subseteq [b]$. A similar argument (omitted here) shows that $[b] \subseteq [a]$. Since $[a] \subseteq [b]$ and $[b] \subseteq [a]$, we have shown that $[a] = [b]$.

(*see text for proof that* (*ii*) *implies* (*iii*) *and* (*iii*) *implies* (*i*))

Partition of a Set

- **Definition**: A *partition* of a set S is a collection of disjoint nonempty subsets of S that have S as their union. In other words, the collection of subsets A_i, where $i \in I$ (where I is an index set), forms a partition of S if and only if
  - $A_i \neq \emptyset$ for $i \in I$,
  - $A_i \cap A_j = \emptyset$ when $i \neq j$,
  - and $\bigcup_{i \in I} A_i = S$



A Partition of a Set

An Equivalence Relation Partitions a Set

- Let R be an equivalence relation on a set A. The union of all the equivalence classes of R is all of A, since an element a of A is in its own equivalence class $[a]_R$. In other words,

$$\bigcup_{a \in A} [a]_R = A$$

- From Theorem 1, it follows that these equivalence classes are either equal or disjoint, so $[a]_R \cap [b]_R = \emptyset$ when $[a]_R \neq [b]_R$.
- Therefore, the equivalence classes form a partition of A, because they split A into disjoint subsets.

An Equivalence Relation Partitions a Set (*continued*)

- **Theorem 2**: Let R be an equivalence relation on a set S. Then the equivalence classes of R form a partition of S. Conversely, given a partition $\{A_i \mid i \in I\}$ of the set S, there is an equivalence relation R that has the sets A_i, $i \in I$, as its equivalence classes.
- **Proof**: We have already shown the first part of the theorem.
- For the second part, assume that $\{A_i \mid i \in I\}$ is a partition of S. Let R be the relation on S consisting of the pairs (x, y) where x and y belong to the same subset A_i in the partition. We must show that R satisfies the properties of an equivalence relation.
  - *Reflexivity*: For every $a \in S$, $(a,a) \in R$, because a is in the same subset as itself.
  - *Symmetry*: If $(a,b) \in R$, then b and a are in the same subset of the partition, so $(b,a) \in R$.
  - *Transitivity*: If $(a,b) \in R$ and $(b,c) \in R$, then a and b are in the same subset of the partition, as are b and c. Since the subsets are disjoint and b belongs to both, the two subsets of the partition must be identical. Therefore, $(a,c) \in R$ since a and c belong to the same subset of the partition.

Partial Orderings

Section 9.6

Section Summary

- Partial Orderings and Partially-ordered Sets
- Lexicographic Orderings
- Hasse Diagrams
- Lattices (*not currently in overheads*)
- Topological Sorting (*not currently in overheads*)

Partial Orderings

- **Definition 1:** A relation *R* on a set S is called a *partial ordering,* or *partial order,* if it is reflexive, antisymmetric, and transitive.
  - A set together with a partial ordering *R* is called a *partially ordered set*, or *poset*, and is denoted by (*S*, *R*). Members of *S* are called *elements* of the poset.

Partial Orderings (*continued*)

- **Example 1:** Show that the "greater than or equal" relation ($\geq$) is a partial ordering on the set of integers.
  - *Reflexivity*: $a \geq a$ for every integer a.
  - *Antisymmetry*: If $a \geq b$ and $b \geq a$, then $a = b$.
  - *Transitivity*: If $a \geq b$ and $b \geq c$, then $a \geq c$.

These properties all follow from the order axioms for the integers. (*See Appendix* 1).

Partial Orderings (*continued*)

- **Example 2:** Show that the the divisibility relation ($\mid$) is a partial ordering on the set of integers.
  - *Reflexivity*: $a \mid a$ for all integers a. (*see Example* 9 *in Section* 9.1)
  - *Antisymmetry*: If a and b are positive integers with $a \mid b$ and $b \mid a$, then $a = b$. (*see Example* 12 *in Section* 9.1)
  - *Transitivity*: Suppose that a divides b and b divides c. Then there are positive integers k and l such that $b = ak$ and $c = bl$. Hence, $c = a(kl)$, so a divides c. Therefore, the relation is transitive.
- $(\mathbf{Z}^+, \mid)$ is a poset.

Partial Orderings (*continued*)

- **Example 3:** Show that the inclusion relation ($\subseteq$) is a partial ordering on the power set of a set S.
  - *Reflexivity*: $A \subseteq A$ whenever A is a subset of S.
  - *Antisymmetry*: If A and B are positive integers with $A \subseteq B$ and $B \subseteq A$, then $A = B$.
  - *Transitivity*: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

The properties all follow from the definition of set inclusion.

Comparability

- **Definition 2:** The elements a and b of a poset $(S, \preccurlyeq)$ are *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$. When a and b are elements of S so that neither $a \preccurlyeq b$ nor $b \preccurlyeq a$, then a and b are called i*ncomparable*.

> The symbol $\preccurlyeq$ is used to denote the relation in any poset.

- **Definition 3:** If $(S, \preccurlyeq)$ is a poset and every two elements of S are comparable, S is called a *totally ordered* or *linearly ordered set*, and $\preccurlyeq$ is called a *total order* or a *linear order.* A totally ordered set is also called a *chain.*
- **Definition 4:** $(S, \preccurlyeq)$ is a well-ordered set if it is a poset such that $\preccurlyeq$ is a total ordering and every nonempty subset of S has a least element.

Lexicographic Order

- **Definition:** Given two posets $(A_1,\preccurlyeq_1)$ and $(A_2,\preccurlyeq_2)$, the *lexicographic ordering* on $A_1 \times A_2$ is defined by specifying that (a_1, a_2) is less than (b_1,b_2), that is,

$$(a_1, a_2) \prec (b_1,b_2),$$

either if $a_1 \prec_1 b_1$ or if $a_1 = b_1$ and $a_2 \prec_2 b_2$.

- **Example:** Consider strings of lowercase English letters. A lexicographic ordering can be defined using the ordering of the letters in the alphabet. This is the same ordering as that used in dictionaries.
  - *discreet* $\prec$ *discrete*, because these strings differ in the seventh position and $e \prec t$.
  - *discreet* $\prec$ *discreetness*, because the first eight letters agree, but the second string is longer.