Discrete Mathematics: Lecture 9

- Last time:
  - Chap 9.4: Closure of relations
- Today:
  - Chap 9.5: Equivalence relations
  - Chap 9.6: Partial orderings

Review of last time

- Closure of relations
- The transitive closure of R equals R^*
- The transitive closure of R equals $R \cup \ldots R^n$ if R is a relation on a set with n elements
- Warshall algorithm

Equivalence relations (等价关系)

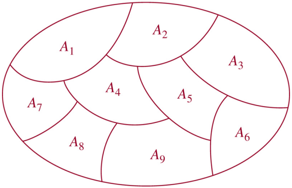
- Definition: A relation on a set A is called an equivalence relation if it is reflexive, symmetric and transitive.
- Definition: Two elements a and b that are related by an equivalence relation are called equivalent, denoted by $a \sim b$.
- Example: Congruence modulo m (模m同余): Let $m \in \mathbf{Z}^+$ with $m > 1$. Let $R = \{(a, b) \mid a, b \in \mathbf{Z}, \text{ and } a \equiv b \pmod{m}\}$.
- Example: Let $n \in \mathbf{Z}^+$ and S is a set of strings. Let R_n be the relation on S such that sRt iff $s = t$, or both s and t have length $\geq n$, and the first n characters of s and t are the same.
- Example: How about the "divides" (整除) relation on $\mathbf{Z}^+$?

Equivalence classes

- Definition: Let R be an equivalence relation on a set A. The equivalence class (等价类) of $a \in A$ wrt R, denoted by $[a]_R$, is the set $\{b \in A \mid aRb\}$.
- When the relation is clear from the context, we simply write $[a]$.
- If $b \in [a]_R$, b is called a representative (代表元) of this class.
- Example: What are $[0]$ and $[1]$ for congruence modulo 4?
- Example: What is $[0111]$ wrt R_3 defined on the last slide?

Partitions

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



- Example: Let $S = \{1, 2, 3, 4, 5, 6\}$. Then $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$, and $A_3 = \{6\}$ form a partition of S.

Equivalence classes and partitions

- Theorem 1: Let R be an equivalence relation on a set A. Let $a, b \in A$. Then aRb iff $[a] = [b]$ iff $[a] \cap [b] \neq \varnothing$.
- 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.
- Example: What is the partition of the integers arising from congruence modulo 4?
- Example: What is the partition of bit strings arising from R_3?

Partial orderings (偏序)

- We often use relations to order some or all of the elements of sets, *e.g.*, $<, \leq$.
- Definition: A relation R on a set S is called a partial ordering or partial order if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a partially ordered set (偏序集), or poset, and is denoted by (S, R).
- Example: $(\mathbf{Z}, \geq)$ is a poset.
- Example: $(\mathbf{Z}^+, |)$ is a poset.
- Example: $(P(S), \subseteq)$ is a poset.

Total order

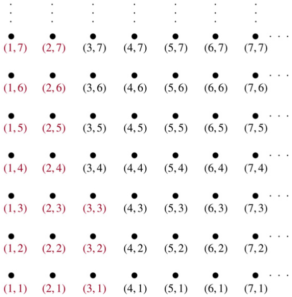
- Notation: We use $a \preccurlyeq b$ to denote that $(a, b) \in R$ in an arbitrary poset. We use $a \prec b$ to denote that $a \preccurlyeq b$ but $a \neq b$.
- Definition: The elements a and b of a poset $(S, \preccurlyeq)$ are called comparable (可比的) if either $a \preccurlyeq b$ or $b \preccurlyeq a$. a and b are called incomparable (不可比的) if neither $a \preccurlyeq b$ nor $b \preccurlyeq a$
- In the poset $(\mathbf{Z}^+, |)$, are 3 and 9 comparable, are 5 and 7 comparable?
- Definition: 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 (全序) or linear order (线序). A totally ordered set is also called a chain (链).
- Example: The poset $(\mathbf{Z}, \geq)$ is totally ordered, but the poset $(\mathbf{Z}^+, |)$ is not.

Well-ordered sets

- Definition: $(S, \preccurlyeq)$ is a well-ordered set (良序集) if it is a totally ordered set and every nonempty subset of S has a least element.
- Example: $(\mathbf{Z}^+, \leq)$ is a well-ordered set, buy $(\mathbf{Z}, \leq)$ is not.
- Theorem: The principle of well-ordered induction (良序归纳原理): Suppose that S is a well-ordered set. Then $P(x)$ is true for all $x \in S$, if INDUCTIVE STEP: For every $y \in S$, if $P(x)$ is true for all $x \in S$ with $x \prec y$, then $P(y)$ is true.
- Remark: We do not need a basis step, because if x_0 is the least element of S, the inductive step tells us that $P(x_0)$ holds.

Lexicographic order (字典序)

- The words in a dictionary are listed in alphabetic, or lexicographic order.
- Definition: Let $(A_1, \preccurlyeq_1)$ and $(A_2, \preccurlyeq_2)$ be two posets. The lexicographic ordering $\preccurlyeq$ on $A_1 \times A_2$ is defined as: $(a_1, a_2) \preccurlyeq (b_1, b_2)$ iff $(a_1, a_2) = (b_1, b_2)$ or $(a_1, a_2) \prec (b_1, b_2)$, where $(a_1, a_2) \prec (b_1, b_2)$ iff $a_1 \prec_1 b_1$ or $a_1 = b_1$ and $a_2 \prec_2 b_2$.
- Example: $(3, 5) \prec (4, 3)$ and $(4, 9) \prec (4, 11)$. The ordered pairs less than $(3, 4)$ are highlighted in the following figure:

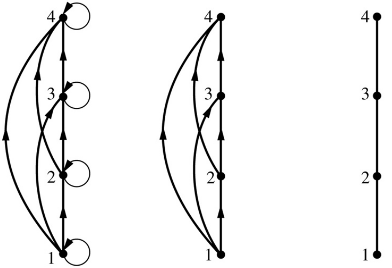


Lexicographic order

- A lexicographic ordering can be defined on the Cartesian product of n posets: $(a_1, a_2, \ldots, a_n) \prec (b_1, b_2, \ldots, b_n)$ iff $a_1 \prec_1 b_1$ or there is an $i > 0$ such that $a_1 = b_1, \ldots, a_i = b_i$, and $a_{i+1} \prec_{i+1} b_{i+1}$.
- Example: $(1, 2, 3, 5) \prec (1, 2, 4, 3)$.
- Lexicographic ordering of strings: $a_1 a_2 \ldots a_m \prec b_1 b_2 \ldots b_n$ iff $(a_1, a_2, \ldots, a_t) \prec (b_1, b_2, \ldots, b_t)$ or $(a_1, a_2, \ldots, a_t) = (b_1, b_2, \ldots, b_t)$ and $m < n$, where $t = min(m, n)$
- Example: $discreet \prec discrete$, $discreet \prec discreetness$, $discrete \prec discretion$,

Motivating Hasse diagrams (哈塞图)

Many edges in the digraph for a finite poset do not have to be shown, *e.g.*, the poset $(\{1, 2, 3, 4\}, \leq)$



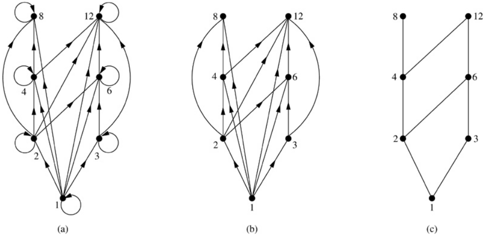
(a) (b) (c)

Hasse diagrams

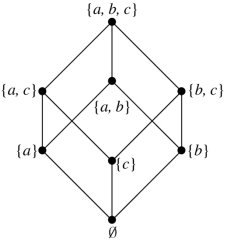
In general, we can represent a finite poset by a Hasse diagram, obtained as follows:

- Start with the digraph for the relation
- Remove all loops
- Remove all edges that can be obtained by transitivity
- Arrange each edge (a, b) so that the initial vertex (起点) a is below the terminal vertex (终点) b, and remove the arrow on the edge

- Example: the poset $(S, |)$, where $S = \{1, 2, 3, 4, 6, 8, 12\}$

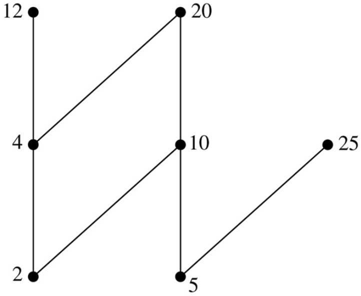


- Example: the poset $(P(S), \subseteq)$, where $S = \{a, b, c\}$



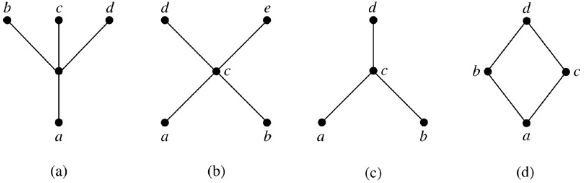
Maximal and minimal elements (极大元与极小元)

- Definition: $a \in S$ is maximal in the poset $(S, \preccurlyeq)$ if there is no $b \in S$ such that $a \prec b$. Similarly, $a \in S$ is minimal in the poset $(S, \preccurlyeq)$ if there is no $b \in S$ such that $b \prec a$.
- Maximal and minimal elements are easy to identify using a Hasse diagram.
- Example: the poset $(S, |)$, where $S = \{2, 4, 5, 10, 12, 20, 25\}$



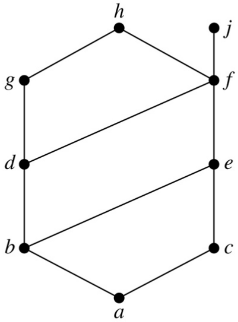
Greatest and least elements (最大元与最小元)

- Definition: $a \in S$ is the greatest element of the poset $(S, \preccurlyeq)$ if $b \preccurlyeq a$ for all $b \in S$. Similarly, $a \in S$ is the least element of the poset $(S, \preccurlyeq)$ if $a \preccurlyeq b$ for all $b \in S$.
- Greatest and least elements are unique when they exist.
- Example: which of the following has a greatest element, and which has a least element:



Upper and lower bounds of a set (集合的上界与下界)

- Definition: Let A be a subset of a poset $(S, \preccurlyeq)$. An upper bound of A is an element $u \in S$ such that $a \preccurlyeq u$ for all $a \in A$. Similarly, a lower bound of A is an element $l \in S$ such that $l \preccurlyeq a$ for all $a \in A$.
- Example: Find the upper and lower bounds of $\{a, b, c\}$, $\{j, h\}$, $\{a, c, d, f\}$:

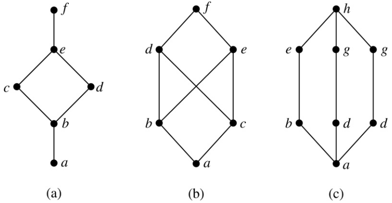


Least upper bound and greatest lower bounds

- Definition: x is the greatest lower bound (最大下界) of A if $x \preccurlyeq a$ for all $a \in A$, and $z \preccurlyeq x$ whenever z is a lower bound of A. x is the least upper bound (最小上界) of A if $a \preccurlyeq x$ for all $a \in A$, and $x \preccurlyeq z$ whenever z is a upper bound of A.
- The greatest lower bound of A is unique when it exists, and we denote it by $glb(A)$. The least upper bound of A is unique when it exists, and we denote it by $lub(A)$.
- Example: Find the glbs and lubs of $\{3, 9, 12\}$ and $\{1, 2, 4, 5, 10\}$, if they exist, in the poset $(\mathbf{Z}^+, |)$?

Lattices (格)

- Definition: A lattice is a poset where every pair of elements has a glb and lub.
- Example: Are the following lattices?



- Example: Is $(\mathbf{Z}^+, |)$ a lattice?
- Example: How about $(\{1,2,3,4,5\}, |)$ and $(\{1,2,4,8,16\}, |)$?
- Example: Is $(P(S), \subseteq)$ a lattice?