Relation, II

李昂生

Discrete Mathematics
U CAS
5, June May, 2018

Outline

General view

- The role of **ordering**
- **Algebra of discrete objects**

Closure of a Relation

Given a set A and a relation on A, the **transitive closure** of R is the $\subseteq$-least relation S such that

i) S transitive

ii) $R \subseteq S$.

Generally,

Definition 1

Let R be a relation on a set A and P be a property. We define the ***P*-*closure* of R** to be the **$\subseteq$-least relation S** satisfying

- S satisfies P
- $R \subseteq S$.

Closes

Given a set A and a relation R on A,

(i) The *reflexive closure* of R is:

$$S = R \cup \{(a,a) \mid a \in A\}. \tag{1}$$

(ii) The *symmetric closure* of R is

$$S = R \cup R^{-1}, \tag{2}$$

where $R^{-1} = \{(b,a) \mid (a,b) \in R\}$.

Paths in Directed Graphs

Definition 2

Let $G = (V, E)$ be a directed graph. A **path** from a to b in G is a sequence of vertices of the following form:

$$a = x_0, x_1, \cdots, x_{l-1}, x_l = b \tag{3}$$

such that for each i with $0 \leq i < l$, (x_i, x_{i+1}) is a directed edge of G, i.e., $(x_i, x_{i+1}) \in E$.

Paths in a Relation on a Set

Let A be a set and R be a relation on A. The notion of paths can be defined for relation R, in which case, the directed edges are the ordered pairs $(a, b) \in R$.

Theorem 3

Let R be a relation on a set A. There is a path of length n from a to b if and only if $(a, b) \in R^n$.

Trivial.

Transitive Closure

Definition 4

Let R be a relation on a set A. Define the **connectivity relation** R^* to be the set of all pairs (a, b) such that there is a path from a to b in G.

By the definition,

$$R^* = \cup_{i \geq 1} R^i. \tag{4}$$

Theorem 5

The transitive closure of R is R^*.

Proof

(i) $R \subseteq R^*$.
(ii) R^* is transitive.
(iii) If S is a transitive relation with $R \subseteq S$, then $R^* \subseteq S$.
R^* is the $\subseteq$-least transitive relation S such that $R \subseteq S$.

Lengths of Paths

Lemma 6

Let A be a set of n elements and R be a relation on A. For any $a, b \in A$, if there is a path from a to b in R, then there is a path of length $\leq n$ from a to b in R.

Suppose to the contrary that for some a and b, there is a path from a to b in R, and that the shortest path from a to b has length $m > n$.
Consider a shortest path of the following form:

$$P: \ a = x_0, x_1, \cdots, x_{m-1}, x_m = b.$$

There are two cases.

Proof- case 1

Case 1 $a = b$.
By the pigeonhole principle, there are i and j such that $1 \leq i < j \leq m$ such that $x_i = x_j$. Therefore,

$$P' : a = x_0, x_1, \cdots, x_i, x_{j+1}, \cdots, x_{m-1}, x_m = b = a,$$

is a path from a to b.
P' has length $m' < m$. A contradiction.

Proof - case 2

Case 2. $a \neq b$.
Subcase 2a. There is an i such that $1 \leq i \leq m-1$ and $x_i = a$ or $x_i = b$.
In either case, there is a path from a to b of length $< m$. A contradiction.
Subcase 2b. Otherwise. Then,

$$\{x_1, \cdots, x_{m-1}\} \subseteq A \setminus \{a, b\}.$$

By the pigeonhole principle, there are i and j such that $1 \leq i < j \leq m-1$ such that $x_i = x_j$. Therefore,

$$a = x_0, x_1, \cdots, x_i, x_{j+1}, \cdots, x_m = b,$$

is a path from a to b, which has length $< m$. A contradiction.

Simple proof

Let

$$P: \quad a = x_1, x_2, \cdots, x_l = b$$

be a path from a to b.
For every $y \in R \setminus \{a, b\}$, if there are $i < j$ such that $x_i = y = x_j$, then
set
P be the path obtained from P by deleting the elements x_k for all k with $i < k \leq j$.
Repeating the procedure we have a path P from a to b such that for every $y \in R \setminus \{a, b\}$, y appears in P at most once. The length of this path is at most $n - 1$.

The Transitive Closure of a Relation

By the Lemma above,

$$R^* = \cup_{i=1}^{n} R^i. \tag{5}$$

In particular,

Theorem 7

Let M_R be the zero-one matrix of the relation R on a set of n elements. Then,

$$M_{R^*} = M_R \vee M_{R^2} \vee \cdots \vee M_{R^n}. \tag{6}$$

Interior Vertices

Let A be a set of n elements and R be a relation on A. Fix an ordering of the elements of A as follows:

$$v_1, v_2, \cdots, v_n,$$

for a path $P: \ a = x_0, x_1, \cdots, x_{m-1}, x_m = b$, we define the *interior vertices* of P to be the set $\{x_1, \cdots, x_{m-1}\}$. We use $I_v(P)$ to denote the interior vertices of P.

Connectivity zero-one matrices using interior vertices

We define the connectivity matrices of R as follows:

1) $W_0 = M_R$.
2) For $k > 0$,

$$W_k = (w_{ij}^{(k)}),$$

where $w_{ij}^{(k)} = 1$ if and only if there is a path P from v_i to v_j such that $I_v(P) \subseteq \{v_1, v_2, \cdots, v_k\}$.

Lemma

Lemma 8

For every k, $0 < k \leq n$, and for all i, j,

$$w_{ij}^{(k)} = w_{ij}^{(k-1)} \vee (w_{ik}^{(k-1)} \wedge w_{kj}^{(k-1)}). \tag{7}$$

Proof

Clearly, if $w_{ij}^{(k-1)} \vee (w_{ik}^{(k-1)} \wedge w_{kj}^{(k-1)}) = 1$, so is $w_{ij}^{(k)}$.
Assume $w_{ij}^{(k)} = 1$.
By definition, there is a path P from v_i to v_j such that $I_v(P) \subseteq \{v_1, v_2, \cdots, v_k\}$.
Let P be the following path

$$v_i = x_0, x_1, \cdots, x_{m-1}, x_m = v_j.$$

There are two cases.

Proof - case 1

Case 1. $v_k \notin I_v(P)$.
This means that $w_{ij}^{(k-1)} = 1$.

Proof - case 2

Case 2. Otherwise.
In this case, $v_k = x_i$ for some i with $1 \leq i \leq m - 1$.
If there are more than one such i's, then let i_0 be the least such i, and i_1 be the greatest such i. Otherwise, then $i_0 = i_1$ be the unique i.
Then,

$$P' : v_i = x_0, x_1, \cdots x_{i_0}, x_{i_1+1}, \cdots , x_{m-1}, x_m = v_j$$

is a path from v_i to v_j such that
$P_1 :\ v_i = x_0, x_1, \cdots x_{i_0}$ is a path from v_i to v_k such that $I_v(P_1) \subseteq \{v_1, \cdots , v_{k-1}\}$, and
$P_2 :\ x_{i_0}, x_{i_1+1}, \cdots , x_{m-1}, x_m = v_j$ is a path from v_k to v_j with $I_v(P_2) \subseteq \{v_1, \cdots , v_{k-1}\}$.
Therefore, $w_{ik}^{(k-1)} = w_{kj}^{(k-1)} = 1$.

Warshall's Algorithm

1. Let $W_0 = M_R$
2. Suppose that W_{k-1} is defined. For every i, j from 1 to n, let

$$w_{ij}^{(k)} = w_{ij}^{(k-1)} \vee (w_{ik}^{(k-1)} \wedge w_{kj}^{(k-1)}).$$

The time complexity:

$$O(n^3).$$

Equivalence Relation

Definition 9

A relation R on a set A is an **equivalence relation**, if R is **reflexive, symmetric and transitive**.

Equivalence Classes

Definition 10

Let R be an equivalence relation on a set A. For an element $a \in A$, the **equivalence class** of a with respect to R is the set of all $x \in A$ such that $(a, x) \in R$. We use $[a]$ to denote the equivalence class of a, where a is called a *representative* of the equivalence class.

Equivalence Relation Implies Partition

Theorem 11

Let R be an equivalence relation on a set A. Then, for any $a, b \in A$, (i), (ii) and (iii) below are equivalent:

(i) $(a, b) \in R$.

(ii) $[a] = [b]$.

(iii) $[a] \cap [b] \neq \emptyset$.

Partition Implies Equivalence Relation

Theorem 12

1. *If R is an equivalence relation on A, then $\{[a] \mid a \in A\}$ is a partition of A.*
2. *If $P = \{A_1, A_2, \cdots, A_m\}$ is a partition of A, then the partition P defines an equivalence relation on A as follows:*
   For $x, y \in A$,

$$(x, y) \in R \iff \exists i, x, y \in A_i.$$

Partially Ordered Set

Definition 13

Given a set S and a relation R on S, we say that R is a *partial ordering*, or *partial order*, or *partially ordered set*, if:

(i) R is reflexive

(ii) R is antisymmetric

(iii) R is transitive

Remark

- In this case, we use $x \leq y$ to denote that $(x, y) \in R$.
- If $x \leq y$ and $x \neq y$, we write $x < y$.

We referred the notion as to: partially ordered set, or partial ordering or partial order. Or we simply call it a *poset*.

Examples

1. $(\mathbb{Z}, \leq)$
2. $(\mathbb{Z}, |)$ where $a|b$ denotes a divides b.
3. $(2^S, \subseteq)$.

Incomparable Relationships

In a partial order, there are incomparable elements.

Definition 14

Let $(A, \leq)$ be a partial order. For $a, b \in A$, we say that a and b are *comparable*, if either $a \leq b$ or $b \leq a$, and *incomparable*, otherwise.

Examples:

1) $(\mathbb{Z}, |)$
   There are integers a and b such that $a \nmid b$ and $b \nmid a$.
1. $(2^A, \subseteq)$
   There are sets X, Y such that $X \not\subseteq Y$ and $Y \not\subseteq X$.

Linear Order

Definition 15

Let $(S, \leq)$ be a partial order. We say that it is a *linear order*, or *totally partial order*, or *totally partial ordering*, if for any $x, y \in S$, either $x \leq y$ or $y \leq x$.

Well-Ordered Set

Definition 16

Let $(A, \leq)$ be a partial order. We say that it is a *well-ordered set*, if:

1) $(A, \leq)$ is a linear order
2) For any set $X \subseteq A$, if $X \neq \emptyset$, then there is an element $x_0 \in X$ such that for any $x \in X$, $x_0 \leq x$, that is, X has a least element.

- $(\mathbb{N}, \leq)$ is a well-ordered set.
- $(\mathbb{Z}, \leq)$ is not a well-ordered set.

The Principle of Well-Ordered Sets

This is the **principle of inductive proofs**.

Theorem 17

(The Principle of Well-Ordered Sets) Let $(S, \leq)$ be a well-ordered set, and P be a property.
Suppose that
For every $x \in S$,

$$(\forall y < x)[P(y) \ \textit{holds}] \to P(x) \ \textit{holds}.$$

Then, for any $x \in S$, $P(x)$ holds.

Proof

Towards a contradiction. Suppose that there is an $x \in S$ such that $P(x)$ fails to hold.
Let X be the set of all $x \in S$ at which P fail to hold.
Since $(S, \leq)$ is well-ordered, X has the least element x_1.
Let x_0 be the least element in S.
Case 1 $x_1 = x_0$.
In this case, there is no $y \in S$ such that $y < x_0$, so the assumption implies that $P(x_0)$ holds. A contradiction.
Case 2. $x_0 < x_1$.
By the choice of x_1, we have that for every $y \in S$, if $y < x_1$, then $P(y)$ holds. By the assumption, $P(x_1)$ holds. A contradiction.
This is actually the principle for inductive proofs.

The Lexicographic Order

Definition 18

Given an alphabet Σ with a fixed order $\{s_1 < s_2 < \cdots < s_k\}$ as they are listed. For any string $x, y \in \Sigma^*$, let $x = a_1 a_2 \cdots a_m$ and $y = b_1 b_2 \cdots b_n$. Then,

(1) We say that x is an *initial segment* of y, if for every i, if $1 \leq i \leq m$, then $a_i = b_i$. We use $x \subseteq y$ to denote that x is an initial segment of y.
If $x \subseteq y$ and $x \neq y$, then we write $x \subset y$.

(2) For $x \not\subseteq y$. We define $x <_{\mathrm{L}} y$, meaning that x is to the left of y, if there is an i such that

- $1 \leq i \leq m$
- $a_i < b_i$
- for every j, if $1 \leq j < i$, $a_j = b_j$.

(3) We define $x \leq y$, if either $x \subseteq y$ or $x <_{\mathrm{L}} y$.
If $x \leq y$ and $x \neq y$, we define $x < y$.

Priority Tree

The lexicographic order defined above gives a priority tree.
Given alphabet Σ with order $s_1 < s_2 < \cdots < s_k$.
The *priority tree T* is built as follows:

1. The root node λ has immediate successors $s_1, s_2, \cdots, s_k$ with the order from left to right as they are listed.
2. For every node $\alpha \in T$, the immediate successors of α are labelled as

$$s_1, s_2, \cdots, s_k$$

with the left to right order as they are listed.

The priority tree T is exactly the lexicographic order.

Hasse Diagrams

Let $(S, \leq)$ be a partial order. For $x, y \in S$, we say that y *covers* x if $x < y$ and there is no z such that $x < z < y$.
The Hasse diagram of a partial order is a simplified graphical representation of the partial as follows:

1. The diagram is growing upwardly.
2. Keep only the edges of covering

Why?
Not interesting!

Greatest and Least Elements

For some poset $(S, \leq)$, there is the greatest and/or the least elements.

- We say that $x \in S$ is the greatest element, if for any $y \in S$, $y \leq x$.
  We use 1 to denote the greatest element of the poset.
- We say that the element s is the least element of the poset, if for any $x \in S$, $s \leq x$.
  In this case, we use 0 to denote the least element of the poset.

The Least Upper Bound

Let $(S, \leq)$ be a poset. For $x, y \in S$, the *least upper bound* of x and y is the element $w \in S$ such that both (1) and (2) below hold:

(1) Both $x \leq w$ and $y \leq w$ hold.

(2) For any $z \in S$, if $x \leq z$ and $y \leq z$, then $w \leq z$.

In this case, we use

$$x \vee y$$

to denote the least upper bound of x and y, if it any.

The Greatest Lower Bound

Let $(S, \leq)$ be a poset. For $x, y \in S$, we define the *greatest lower bound* of x and y, if any, to be the element $w \in S$ satisfying the following:

1. Both $w \leq x$ and $w \leq y$ hold
2. For any $z \in S$, if $z \leq w$ and $z \leq y$, then $z \leq w$.

We use

$$x \wedge y$$

to denote the greatest lower bound of x and y, if any.

Lattices

Definition 19

Let $(S, \leq)$ be a partial order. We say that $(L, \leq)$ is a *lattice*, if for any $x, y \in L$,

1) $x \vee y$ exists.
2) $x \wedge y$ exists.

In this case, we use $\langle L, \leq, \vee, \wedge \rangle$ to denote the lattice. Furthermore, if the greatest and the least elements exist, we write

$$\langle L, \leq, \vee, \wedge, 0, 1 \rangle.$$

Examples

1. $(\mathbb{N}, |)$ is a lattice
   $\vee$ and $\wedge$ are the least common multiple and the greatest common divisor, respectively.
2. $\langle 2^A, \subseteq, \cup, \cap, 0, 1\rangle$ is a lattice.
   $0 = \emptyset$, and $1 = A$. $\cup$ and $\cap$ are the set union and meet, respectively.
3. $(\Sigma^*, \subseteq)$ is not a lattice where $\subseteq$ is the relation of initial segment.
   The $\wedge$ exists, but $\vee$ fails to exist.

Laws of Lattices

Theorem 20

Let $\langle L, \leq, \vee, \wedge \rangle$ be a lattice. Then, for any $x, y, z \in L$,

1. *(Commutative laws)*
$$x \wedge y = y \wedge x, \quad x \vee y = y \vee x.$$
2. *(Associative laws)*
$$(x \wedge y) \wedge z = x \wedge (y \wedge z), \quad (x \vee y) \vee z = x \vee (y \vee z).$$
3. *(Absorptive laws)*
$$x \wedge (x \vee y) = x, \quad x \vee (x \wedge y) = x.$$
4. *(Idempotent laws)*
$$x \wedge x = x, \quad x \vee x = x.$$

Lattice $\langle L, \leq, \vee, \wedge, 0, 1\rangle$

In a lattice $\langle L, \leq, \vee, \wedge, 0, 1\rangle$ with 0 and 1,, for any $x \in L$,

1. $x \vee 1 = 1$
2. $x \wedge 1 = x$
3. $x \vee 0 = x$
4. $x \wedge 0 = 0$.

Generally, if $x \leq y$, then

$$x \vee y = y$$

$$x \wedge y = x$$

Distributive Lattices

We say that a lattice $\langle L, \leq, \vee, \wedge \rangle$ is *distributive*, if for any $x, y, z \in L$,

(1)

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

(2)

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

Complement in a Lattice

Given a lattice $\langle L, \leq, \vee, \wedge, 0, 1\rangle$, for $a \in L$ and $b \in L$, if $0 < a, b < 1$, we say that b is the *complement* of a, if:

(i)
$$a \vee b = 1,$$

(ii)
$$a \wedge b = 0.$$

The Problem

The topological sorting is to **extend** a poset to a linear order, or totally partial order.
Given a poset $(S, \leq)$, find a partial order $\leq_{\mathrm{T}}$ such that for any $x, y \in S$,

-
$$x \leq y \Rightarrow x \leq_{\mathrm{T}} y,$$
  and
- x and y are $\leq_{\mathrm{T}}$ comparable

Minimal Element

Lemma 21

Every finite nonempty poset $(S, \leq)$ *has at least one minimal element.*

The Topological Sorting Algorithm

Given a poset $(S, \leq)$ of n elements,

1. Let a_1 be a minimal element of $S_0 = S$
   Suppose that $a_1, \cdots, a_k$ are chosen. Let
   $S_k = S \setminus \{a_1, \cdots, a_k\}$.
2. Let a_{k+1} be a minimal element in S_k.
3. Fir each i, define

$$a_i \leq_{\mathrm{T}} a_{i+1}.$$

Proof

Clearly, $\leq_{\mathrm{T}}$ is a total ordering.
We show that $\leq_{\mathrm{T}}$ extends $\leq$.
Suppose to the contrary the result fails to hold. Then there are $x < y$ and $i < j$ such that $x = a_j$ and $y = a_i$. By the definition of the a_i's, when we define $a_i = y$ at step i, $x \in S_{i-1}$. By the choice of $a_i = y$, there is no $z \in S_{i-1}$ such that $z < y$. This is a contradiction.

Exercises

1. Let $p(n)$ be the number of different equivalence relation on a set of n elements. Show that $p(n)$ satisfies the recurrence relation:

$$
\begin{aligned}
p(n) &= \sum_{j=0}^{n-1} \binom{n-1}{j} p(n-j-1), \\
P(0) &= 1.
\end{aligned}
$$

2. Show that every finite partial order can be partitioned into k chains, where k is the largest number of elements in an anti-chain in the partial order.
   Definition Given a partial order P and a subset $S \subset P$, we say that S is a chain of P, if every two elements in S are comparable in P, and that S is an anti-chain of P, if every two elements in S are incomparable in P.

谢谢！