CS 207: Discrete Structures

Instructor : S. Akshay

Aug 11, 2015

Lecture 11 – Basic mathematical structures: lattices and on to counting

Quiz tomorrow (Wednesday, 12^{th} August)

- Venue: F.C. Kohli auditorium, Kresit
- Duration: 55min.
- Time: 08:30am to 09:25am.
- Syllabus: Till whatever was covered last Thursday.
- Closed book, closed notes.

Minimal and maximal elements

Let $(S, \preceq)$ be a poset.

- An element $a \in S$ is called minimal if, $b \preceq a$ implies $b = a$.
- An element $a \in S$ is called maximal if, $a \preceq b$ implies $a = b$.

Minimal and maximal elements

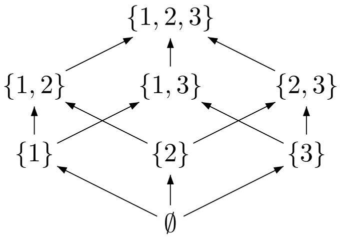
Let $(S, \preceq)$ be a poset.

- An element $a \in S$ is called minimal if, $b \preceq a$ implies $b = a$.
- An element $a \in S$ is called maximal if, $a \preceq b$ implies $a = b$.
- An element $a \in S$ is called the least element of S if $a \preceq b$ for all $b \in S$.
- An element $a \in S$ is called the greatest element of S if $b \preceq a$ for all $b \in S$.

Minimal and maximal elements

Let $(S, \preceq)$ be a poset.

- An element $a \in S$ is called minimal if, $b \preceq a$ implies $b = a$.
- An element $a \in S$ is called maximal if, $a \preceq b$ implies $a = b$.
- An element $a \in S$ is called the least element of S if $a \preceq b$ for all $b \in S$.
- An element $a \in S$ is called the greatest element of S if $b \preceq a$ for all $b \in S$.



Least upper bounds and greatest lower bounds

Let $(S, \preceq)$ be a poset and $A \subseteq S$.

- $u \in S$ (resp. $l \in S$) is called an upper bound (resp. lower bound) of A iff $a \preceq u$ (resp. $l \preceq a$) for all $a \in A$.

Least upper bounds and greatest lower bounds

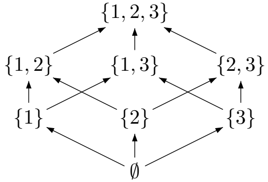
Let $(S, \preceq)$ be a poset and $A \subseteq S$.

- $u \in S$ (resp. $l \in S$) is called an upper bound (resp. lower bound) of A iff $a \preceq u$ (resp. $l \preceq a$) for all $a \in A$.
- $u \in S$ is called the least upper bound of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is called the greatest lower bound of A if it is an lower bound of A and is greater than every other lower bound.

Least upper bounds and greatest lower bounds

Let $(S, \preceq)$ be a poset and $A \subseteq S$.

- $u \in S$ (resp. $l \in S$) is called an upper bound (resp. lower bound) of A iff $a \preceq u$ (resp. $l \preceq a$) for all $a \in A$.
- $u \in S$ is called the least upper bound of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is called the greatest lower bound of A if it is an lower bound of A and is greater than every other lower bound.



Least upper bounds and greatest lower bounds

Let $(S, \preceq)$ be a poset and $A \subseteq S$.

- $u \in S$ (resp. $l \in S$) is called an upper bound (resp. lower bound) of A iff $a \preceq u$ (resp. $l \preceq a$) for all $a \in A$.
- $u \in S$ is called the least upper bound of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is called the greatest lower bound of A if it is an lower bound of A and is greater than every other lower bound.

Some properties:

- The lub/glb of a subset A in S, if it exists, is unique.
- If the lub/glb of $A \subseteq S$ belongs to A, then it is the greatest/least element of A.
- Every nonempty subset A of a totally ordered set S has a glb/lub.

Least upper bounds and greatest lower bounds

Let $(S, \preceq)$ be a poset and $A \subseteq S$.

- $u \in S$ (resp. $l \in S$) is called an upper bound (resp. lower bound) of A iff $a \preceq u$ (resp. $l \preceq a$) for all $a \in A$.
- $u \in S$ is called the least upper bound of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is called the greatest lower bound of A if it is an lower bound of A and is greater than every other lower bound.

Some properties:

- The lub/glb of a subset A in S, if it exists, is unique.
- If the lub/glb of $A \subseteq S$ belongs to A, then it is the greatest/least element of A.
- Every nonempty subset A of a finite totally ordered set S has a glb/lub.

Least upper bounds and greatest lower bounds

Let $(S, \preceq)$ be a poset and $A \subseteq S$.

- $u \in S$ (resp. $l \in S$) is called an upper bound (resp. lower bound) of A iff $a \preceq u$ (resp. $l \preceq a$) for all $a \in A$.

An aside: Theorem (Zorn's lemma)

Given a poset $(S, \preceq)$, if every non-empty chain in S has an upper-bound in S, then S has some maximal element.

Lattices and complete lattices

- A lattice is a poset in which every pair of elements has both a lub and a glb (in the set), i.e., $\forall x, y \in S$, there exists $l, u \in S$ such that l is the glb and u is the lub of $\{x, y\}$.
- A complete lattice is a poset in which any subset of elements has both a lub and a glb (in the set), i.e., $\forall S' \subseteq S$, there exists $l, u \in S$ such that l is the glb and u is the lub of S'.

Some exercises:

1. Which totally ordered sets are lattices?
2. Does a subset of a finite lattice always have a lub/glb?
3. Does a finite subset of any lattice always have a lub/glb? What about infinite subsets?
4. Is every lattice is complete?
5. Does a complete lattice always have greatest/least elements?

A fixed point theorem

- Given two posets $(S, \preceq_s)$ and $(T, \preceq_T)$, $f : S \to T$ is order-preserving or monotonic if for all $a, b \in S$, $a \preceq_S b$ implies $f(a) \preceq_T f(b)$.

A fixed point theorem

- Given two posets $(S, \preceq_s)$ and $(T, \preceq_T)$, $f : S \to T$ is order-preserving or monotonic if for all $a, b \in S$, $a \preceq_S b$ implies $f(a) \preceq_T f(b)$.
- For $f : S \to S$, $x \in S$ is a fixed point of f if $f(x) = x$.

A fixed point theorem

- Given two posets $(S, \preceq_s)$ and $(T, \preceq_T)$, $f : S \to T$ is order-preserving or monotonic if for all $a, b \in S$, $a \preceq_S b$ implies $f(a) \preceq_T f(b)$.
- For $f : S \to S$, $x \in S$ is a fixed point of f if $f(x) = x$.

Theorem (Tarski's fixed point theorem)

Let $(S, \preceq)$ be a complete lattice and $f : S \to S$ be a monotonic function. Then the set of fixed points of f is a (non-empty) complete lattice.

A fixed point theorem

- Given two posets $(S, \preceq_s)$ and $(T, \preceq_T)$, $f : S \to T$ is order-preserving or monotonic if for all $a, b \in S$, $a \preceq_S b$ implies $f(a) \preceq_T f(b)$.
- For $f : S \to S$, $x \in S$ is a fixed point of f if $f(x) = x$.

Theorem (Tarski's fixed point theorem)

Let $(S, \preceq)$ be a complete lattice and $f : S \to S$ be a monotonic function. Then the set of fixed points of f is a (non-empty) complete lattice. Thus, there exists a least fixed point of f in S.

A fixed point theorem

- Given two posets $(S, \preceq_s)$ and $(T, \preceq_T)$, $f : S \rightarrow T$ is order-preserving or monotonic if for all $a, b \in S$, $a \preceq_S b$ implies $f(a) \preceq_T f(b)$.
- For $f : S \rightarrow S$, $x \in S$ is a fixed point of f if $f(x) = x$.

Theorem (Tarski's fixed point theorem)

Let $(S, \preceq)$ be a complete lattice and $f : S \rightarrow S$ be a monotonic function. Then the set of fixed points of f is a (non-empty) complete lattice. Thus, there exists a least fixed point of f in S.

- Important result with several applications in many domains of mathematics and CS, including formal semantics of programming languages, program verification.

A fixed point theorem

- Given two posets $(S, \preceq_s)$ and $(T, \preceq_T)$, $f : S \to T$ is order-preserving or monotonic if for all $a, b \in S$, $a \preceq_S b$ implies $f(a) \preceq_T f(b)$.
- For $f : S \to S$, $x \in S$ is a fixed point of f if $f(x) = x$.

Theorem (Tarski's fixed point theorem)

Let $(S, \preceq)$ be a complete lattice and $f : S \to S$ be a monotonic function. Then the set of fixed points of f is a (non-empty) complete lattice. Thus, there exists a least fixed point of f in S.

- Important result with several applications in many domains of mathematics and CS, including formal semantics of programming languages, program verification.
- Finite lattices and boolean algebra have a strong link.

Summary till now

Course Outline

1. Proofs and structures
2. Counting and combinatorics
3. Introduction to graph theory
4. Elements of number theory
5. Elements of group theory and abstract algebra

Summary till now

Course Outline

1. Proofs and structures
   - Propositions, predicates
   - Proofs and proof techniques: contradiction, contrapositive, (strong) induction, well-ordering principle, diagonalization.
   - Basic mathematical structures: (finite and infinite) sets, functions, relations.
   - Relations: equivalence relations, partial orders, lattices
   - Some applications
2. Counting and combinatorics
3. Introduction to graph theory
4. Elements of number theory
5. Elements of group theory and abstract algebra

Summary till now

Course Outline

1. Proofs and structures
   - Propositions, predicates
   - Proofs and proof techniques: contradiction, contrapositive, (strong) induction, well-ordering principle, diagonalization.
   - Basic mathematical structures: (finite and infinite) sets, functions, relations.
   - Relations: equivalence relations, partial orders, lattices
   - Some applications
     - Functions: To compare infinite sets
     - Using diagonalization to prove impossibility results.
     - Equivalences: Defining "like" partitions.
     - Posets: Topological sort, (parallel) task scheduling,
     - Lattices: Knaster-Tarski fixed point theorem.
2. Counting and combinatorics
3. Introduction to graph theory
4. Elements of number theory
5. Elements of group theory and abstract algebra

Summary till now

Course Outline

1. Proofs and structures
   - Propositions, predicates
   - Proofs and proof techniques: contradiction, contrapositive, (strong) induction, well-ordering principle, diagonalization.
   - Basic mathematical structures: (finite and infinite) sets, functions, relations.
   - Relations: equivalence relations, partial orders, lattices
   - Some applications
2. Counting and combinatorics
3. Introduction to graph theory
4. Elements of number theory
5. Elements of group theory and abstract algebra

Next chapter: Counting and Combinatorics

Topics to be covered

- Basics of counting
- Subsets, partitions, Permutations and combinations
- Pigeonhole Principle and its extensions
- Recurrence relations and generating functions
- Principle of Inclusion and Exclusion and its applications

Introduction to combinatorics

Does it really need an introduction

Introduction to combinatorics

Does it really need an introduction

- Enumerative combinatorics: counting combinatorial/discrete objects e.g., sets, numbers, structures...
- Existential combinatorics: show that there exist some combinatorial "configurations".
- Constructive combinatorics: construct interesting configurations...

Simple examples...

- How many reflexive relations are there on a set A of size n?

- How many subsets does a set A of n elements have?

Simple examples...

- How many reflexive relations are there on a set A of size n?
  - Reflexive relations are ordered pairs of which there are n^2.
- How many subsets does a set A of n elements have?

Simple examples...

- How many reflexive relations are there on a set A of size n?
  - Reflexive relations are ordered pairs of which there are n^2.
  - Of these, all pairs (a, a) have be present.
  - Of the remaining, we can choose any of them to be in or out.
  - there are $n^2 - n$ of them, so how many choices?
  - We use the so-called "product principle"...
- How many subsets does a set A of n elements have?

Simple examples...

- How many reflexive relations are there on a set A of size n?

- How many subsets does a set A of n elements have?
  - Product principle: two choices for each element, hence $2 \cdot 2 \cdots 2 \cdot 2$ (n-times).
  - Bijection: between $\mathcal{P}(X)$ and $\{0, 1\}$ (characteristic vector).
  - Induction: Since we already know the answer!
  - Recurrence: $F(n) = 2 \cdot F(n-1)$, $F(0) = 1$. But how to solve this recursion?
  - Sum principle: Subsets of size 0 + subsets of size 1 + ... + subsets of size n = Total number of subsets.
  - others?

Simple examples...

- How many reflexive relations are there on a set A of size n?

- How many subsets does a set A of n elements have?
  - Product principle: two choices for each element, hence $2 \cdot 2 \cdots 2 \cdot 2$ (n-times).
  - Bijection: between $\mathcal{P}(X)$ and $\{0, 1\}$ (characteristic vector).
  - Induction: Since we already know the answer!
  - Recurrence: $F(n) = 2 \cdot F(n-1)$, $F(0) = 1$. But how to solve this recursion?
  - Sum principle: Subsets of size 0 + subsets of size 1 + ... + subsets of size n = Total number of subsets.
  - others?
- How many subsets of size k does a set of n elements have?