CS 105: Department Introductory Course on Discrete Structures

Instructor : S. Akshay

Sep 12, 2025

Lecture 12 – Basic structures: lattices, and then onto next Module.

Logistics

Midsem

- Saturday 20th
- More announcements on Piazza reagarding seating and venue.
- Syllabus: all till last lecture including posets, chains, Mirsky's Theorem. No lattices.

Logistics

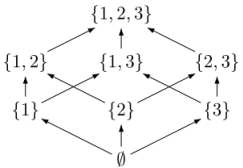
Midsem

- Saturday 20th
- More announcements on Piazza reagarding seating and venue.
- Syllabus: all till last lecture including posets, chains, Mirsky's Theorem. No lattices.

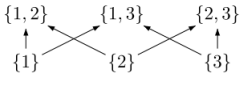
Optional basics help session

- Tomorrow, Saturday 3pm
- Last organized help session before midsem

Minimal and maximal elements



Poset $P_1 = (S_1, \subseteq)$
where $S_1 = \mathcal{P}(\{1, 2, 3\})$

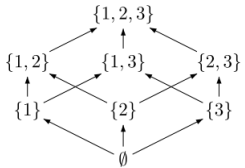


Poset $P_2 = (S_2, \subseteq)$
where $S_2 = \mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}$

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

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

Minimal and maximal elements



Poset $P_1 = (S_1, \subseteq)$
where $S_1 = \mathcal{P}(\{1, 2, 3\})$

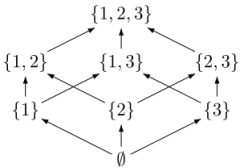


Poset $P_2 = (S_2, \subseteq)$
where $S_2 = \mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}$

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

- $a \in S$ is minimal in S if $\forall b \in S, b \preceq a \implies b = a$
- $a \in S$ is maximal in S if $\forall b \in S, a \preceq b \implies a = b$.
- $a \in S$ is least/minimum element of S if $\forall b \in S, a \preceq b$
- $a \in S$ is greatest/maximum element of S if $\forall b \in S, b \preceq a$.

Minimal and maximal elements



Poset $P_1 = (S_1, \subseteq)$
where $S_1 = \mathcal{P}(\{1, 2, 3\})$



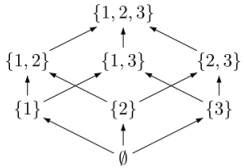
Poset $P_2 = (S_2, \subseteq)$
where $S_2 = \mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}$

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

- $a \in S$ is minimal in S if $\forall b \in S, b \preceq a \implies b = a$
- $a \in S$ is maximal in S if $\forall b \in S, a \preceq b \implies a = b$.
- $a \in S$ is least/minimum element of S if $\forall b \in S, a \preceq b$
- $a \in S$ is greatest/maximum element of S if $\forall b \in S, b \preceq a$.

Examples: $\emptyset$ is a minimal and the minimum element in P_1, $\{1\}, \{2\}, \{3\}$ are all minimal elements in P_2, but P_2 does not have any minimum element.

Minimal and maximal elements



Poset $P_1 = (S_1, \subseteq)$
where $S_1 = \mathcal{P}(\{1, 2, 3\})$



Poset $P_2 = (S_2, \subseteq)$
where $S_2 = \mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}$

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

- $a \in S$ is minimal in S if $\forall b \in S, b \preceq a \implies b = a$
- $a \in S$ is maximal in S if $\forall b \in S, a \preceq b \implies a = b$.
- $a \in S$ is least/minimum element of S if $\forall b \in S, a \preceq b$
- $a \in S$ is greatest/maximum element of S if $\forall b \in S, b \preceq a$.

Examples: $\emptyset$ is a minimal and the minimum element in P_1, $\{1\}, \{2\}, \{3\}$ are all minimal elements in P_2, but P_2 does not have any minimum element.

Exercise: What are the maximal/maximum elements in P_1, P_2?

Least upper bounds and greatest lower bounds

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

- $u \in S$ is called an upper bound of A iff $a \preceq u$ for all $a \in A$.

Least upper bounds and greatest lower bounds

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

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

Least upper bounds and greatest lower bounds

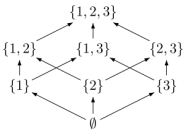
Let $(S, \preceq)$ be a poset and $A \subseteq S$.

- $u \in S$ (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 the least upper bound (lub) of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is the greatest lower bound (glb) of A if it is a lower bound of A and is greater than every other lower bound.

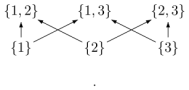
Least upper bounds and greatest lower bounds

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 the least upper bound (lub) of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is the greatest lower bound (glb) of A if it is a lower bound of A and is greater than every other lower bound.



Poset $P_1 = (S_1, \subseteq)$
where $S_1 = \mathcal{P}(\{1, 2, 3\})$

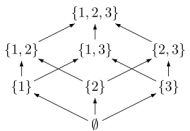


Poset $P_2 = (S_2, \subseteq)$
where $S_2 = \mathcal{P}(\{1, 2, 3\}) \setminus \{\emptyset, \{1, 2, 3\}\}$

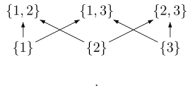
Least upper bounds and greatest lower bounds

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 the least upper bound (lub) of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is the greatest lower bound (glb) of A if it is a lower bound of A and is greater than every other lower bound.



Poset $P_1 = (S_1, \subseteq)$
where $S_1 = \mathcal{P}(\{1,2,3\})$



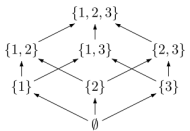
Poset $P_2 = (S_2, \subseteq)$
where $S_2 = \mathcal{P}(\{1,2,3\}) \setminus \{\emptyset, \{1,2,3\}\}$

- Let $A = \{\{1\}, \{2\}\}$. Then $\{1,2\}, \{1,2,3\}$ are upper bounds of A in P_1 and $\{1,2\}$ is the lub of A.

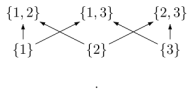
Least upper bounds and greatest lower bounds

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 the least upper bound (lub) of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is the greatest lower bound (glb) of A if it is a lower bound of A and is greater than every other lower bound.



Poset $P_1 = (S_1, \subseteq)$
where $S_1 = \mathcal{P}(\{1,2,3\})$



Poset $P_2 = (S_2, \subseteq)$
where $S_2 = \mathcal{P}(\{1,2,3\}) \setminus \{\emptyset, \{1,2,3\}\}$

- Let $A = \{\{1\}, \{2\}\}$. Then $\{1,2\}, \{1,2,3\}$ are upper bounds of A in P_1 and $\{1,2\}$ is the lub of A. In P_2, is there an lub for S_2?

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 the least upper bound (lub) of A if it is an upper bound of A and is less than every other upper bound.
- $l \in S$ is the greatest lower bound (glb) of A if it is a lower bound of A and is greater than every other lower bound.

Some Obervations (Exercise: Prove it!)

- 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.

Lattices

Definition

- 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 $\{x, y\}$.

Lattices

Definition

- 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 $\{x, y\}$.

- $(\mathcal{P}(S), \subseteq)$ is a lattice.

Lattices

Definition

- 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 $\{x, y\}$.

- $(\mathcal{P}(S), \subseteq)$ is a lattice.
- What about $(\{2, 4, 5, 10, 12, 20, 25\}, |), (\{1, 2, 4, 8, 16\}, |), (\mathbb{Z}^+, |)$?

Lattices

Definition

- 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 $\{x, y\}$.

- $(\mathcal{P}(S), \subseteq)$ is a lattice.
- What about $(\{2, 4, 5, 10, 12, 20, 25\}, |), (\{1, 2, 4, 8, 16\}, |), (\mathbb{Z}^+, |)$?

Applications of Lattices

- Models of information flow –

Lattices

Definition

- 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 $\{x, y\}$.

- $(\mathcal{P}(S), \subseteq)$ is a lattice.
- What about $(\{2, 4, 5, 10, 12, 20, 25\}, |), (\{1, 2, 4, 8, 16\}, |), (\mathbb{Z}^+, |)$?

Applications of Lattices

- Models of information flow – think security clearence.

Lattices

Definition

- 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 $\{x, y\}$.

- $(\mathcal{P}(S), \subseteq)$ is a lattice.
- What about $(\{2, 4, 5, 10, 12, 20, 25\}, |), (\{1, 2, 4, 8, 16\}, |), (\mathbb{Z}^+, |)$?

Applications of Lattices

- Models of information flow – think security clearence.
- Finite lattices have a strong link with Boolean Algebra

Lattices

Definition

- 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 $\{x, y\}$.
- $(\mathcal{P}(S), \subseteq)$ is a lattice.
- What about $(\{2, 4, 5, 10, 12, 20, 25\}, |), (\{1, 2, 4, 8, 16\}, |), (\mathbb{Z}^+, |)$?

Applications of Lattices

- Models of information flow – think security clearence.
- Finite lattices have a strong link with Boolean Algebra
- Several other applications in many domains of mathematics and CS, including formal semantics of programming languages, program verification.

Summary till now

Course Outline

1. Proofs and reasoning
2. Basic discrete structures
3. Counting and combinatorics
4. Introduction to graph theory

Summary till now

Course Outline

1. Proofs and reasoning
   - Propositions, predicates
   - Proofs and proof techniques: contradiction, contrapositive, (strong) induction, well-ordering principle, diagonalization.
2. Basic discrete structures
3. Counting and combinatorics
4. Introduction to graph theory

Summary till now

Course Outline

1. Proofs and reasoning
   - Propositions, predicates
   - Proofs and proof techniques: contradiction, contrapositive, (strong) induction, well-ordering principle, diagonalization.
2. Basic discrete structures
   - (finite and infinite) sets
   - Functions: injections, surjections, bijections
   - 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
3. Counting and combinatorics
4. Introduction to graph theory

Summary till now

Course Outline

1. Proofs and reasoning
   - Propositions, predicates
   - Proofs and proof techniques: contradiction, contrapositive, (strong) induction, well-ordering principle, diagonalization.
2. Basic discrete structures
   - (finite and infinite) sets
   - Functions: injections, surjections, bijections
   - Relations: equivalence relations, partial orders, lattices
   - Some applications
3. Counting and combinatorics
4. Introduction to graph theory

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

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 and principles...

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

Simple examples and principles...

- 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 n pairs of (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 2^{n^2-n} of them.
  - We used the so-called "product principle"...

Simple examples and principles...

- 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 n pairs of (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 2^{n^2-n} of them.
  - We used the so-called "product principle"...

The product principle

If there are n_1 ways of doing something and n_2 ways of doing another thing, then there are $n_1 \cdot n_2$ ways of performing both actions.

Simple examples and principles...

- How many reflexive relations are there on a set A of size n?
- How many functions are there from a set of size n to itself?
- How many subsets does a set A of n elements have?

Simple examples and principles...

- How many reflexive relations are there on a set A of size n?
- How many functions are there from a set of size n to itself?
- 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 n-length sequences over $\{0, 1\}$ (characteristic vector).
  - Induction: Since we already know the answer!
  - Recurrence: $F(n) = 2 \cdot F(n-1), F(0) = 1$. solve it?
  - Sum principle: Subsets of size 0 + subsets of size 1 + ... + subsets of size n = Total number of subsets.

Simple examples and principles...

- How many reflexive relations are there on a set A of size n?
- How many functions are there from a set of size n to itself?
- 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 n-length sequences over $\{0, 1\}$ (characteristic vector).
  - Induction: Since we already know the answer!
  - Recurrence: $F(n) = 2 \cdot F(n-1), F(0) = 1$. solve it?
  - Sum principle: Subsets of size 0 + subsets of size 1 + ... + subsets of size n = Total number of subsets.

Sum Principle

If something can be done in n_1 or n_2 ways such that none of the n_1 ways is the same as any of the n_2 ways, then the total number of ways to do this is $n_1 + n_2$.

Simple examples and principles...

- How many reflexive relations are there on a set A of size n?
- How many functions are there from a set of size n to itself?
- 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 n-length sequences over $\{0, 1\}$ (characteristic vector).
  - Induction: Since we already know the answer!
  - Recurrence: $F(n) = 2 \cdot F(n-1), F(0) = 1$. solve it?
  - Sum principle: Subsets of size 0 + subsets of size 1 + ... + subsets of size n = Total number of subsets.
- But, how many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.

Simple examples and principles...

- How many reflexive relations are there on a set A of size n?
- How many functions are there from a set of size n to itself?
- 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 n-length sequences over $\{0, 1\}$ (characteristic vector).
  - Induction: Since we already know the answer!
  - Recurrence: $F(n) = 2 \cdot F(n-1), F(0) = 1$. solve it?
  - Sum principle: Subsets of size 0 + subsets of size 1 + ... + subsets of size n = Total number of subsets.
- But, how many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.
- We all know(?) that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Prove it!

Permutations and combinations

Binomial Coefficients. Let n, k be integers s.t., $n \geq k \geq 0$.

How many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.

One proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is as follows:

Permutations and combinations

Binomial Coefficients. Let n, k be integers s.t., $n \geq k \geq 0$.

How many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.

One proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is as follows: Let us count the number of "ordered" subsets of size k.

Permutations and combinations

Binomial Coefficients. Let n, k be integers s.t., $n \geq k \geq 0$.

How many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.

One proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is as follows: Let us count the number of "ordered" subsets of size k.

- No. of ordered subsets of size $k = n \cdot (n-1) \cdots (n-k+1)$.

Permutations and combinations

Binomial Coefficients. Let n, k be integers s.t., $n \geq k \geq 0$.

How many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.

One proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is as follows: Let us count the number of "ordered" subsets of size k.

- No. of ordered subsets of size k= $n \cdot (n-1) \cdots (n-k+1)$.
- No. of ordered subsets of size k = (no. of unordered subsets)$\times$(no. of ways to order them)=$\binom{n}{k} \times k!$.

Permutations and combinations

Binomial Coefficients. Let n, k be integers s.t., $n \geq k \geq 0$.

How many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.

One proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is as follows: Let us count the number of "ordered" subsets of size k.

- No. of ordered subsets of size k= $n \cdot (n-1) \cdots (n-k+1)$.
- No. of ordered subsets of size k = (no. of unordered subsets)$\times$(no. of ways to order them)=$\binom{n}{k} \times k!$.
- Equate them! Principle of double counting.
  - if you can't count something, count something else and count it twice over!

Permutations and combinations

Binomial Coefficients. Let n, k be integers s.t., $n \geq k \geq 0$.

How many subsets of size k does a set of n elements have? This number, denoted $\binom{n}{k}$, is called a binomial coefficient.

One proof of $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is as follows: Let us count the number of "ordered" subsets of size k.

- No. of ordered subsets of size k= $n \cdot (n-1) \cdots (n-k+1)$.
- No. of ordered subsets of size k = (no. of unordered subsets)$\times$(no. of ways to order them)=$\binom{n}{k} \times k!$.
- Equate them! Principle of double counting.

Permutations and combinations

- No. of k-size subsets of set of size n = No. of k-combinations of a set of n (distinct) elements = $\binom{n}{k}$.
- No. of k-size ordered subsets of set of size n = No. of k-permutations of a set of n (distinct) elements.

Simple examples to illustrate “double counting”

Prove the following identities (by only using double counting!)

1. $\sum_{k=0}^{n} \binom{n}{k} = 2^n.$
2. $\binom{n}{k} = \binom{n}{n-k}.$
3. $k\binom{n}{k} = n\binom{n-1}{k-1}$
4. $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Simple examples to illustrate "double counting"

Prove the following identities (by only using double counting!)

1. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.
2. $\binom{n}{k} = \binom{n}{n-k}$.
3. $k\binom{n}{k} = n\binom{n-1}{k-1}$
4. $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

The latter two are in fact recursive definitions for $\binom{n}{k}$. What are the boundary conditions?

A more interesting example with double counting

Handshake Lemma

At a meeting with n people, the number of people who shake hands an odd number of times is even.

What will you count here?