Theory of Computation

Tutorial - Math Preliminaries

Cesare Spinoso-Di Piano

Plan for today

1. Introduction
2. Review of set theory
3. Review of graph theory
4. Review of (some) proof techniques

Introduction

Expectations

- This is yet another theoretical computer science resource to study from.
- PDFs of these slides and additional notes/exercises on my website https://cesare-spinoso.github.io/teaching/theoretical_cs
- Some exercises will have typed solutions and others will have video solutions (and others might just have no solutions).
- If there's anything you think could be added or improved, don't hesitate to let me know (submit an issue on GitHub).

Review of set theory

Definition of a set

Definition. A set S is an unordered, well-defined collection of distinct elements.

Example 1. $S_1 = \{1, 2, 8, \textit{twenty}, \#, **, 56\}$ - *Finite* set.

Example 2. $S_2 = \{1, 2, 3, ..., 49\}$.

Example 3. $S_2 = \{n : \text{n is an integer greater than 23}\}$.

Example 4. $S_3 = \{n \in \mathbb{Z} : n \geq 0 \ \ \& \ \ n = 2k\}$ - *Infinite* set of ...?

Example 5. What do the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$ represent?

Example 6. $S_4 = \{n^3 - 3 : n \in \mathbb{Z} \ \ \& \ \ 0 \leq n \leq 27\}$ - What's the smallest number in this set? Is it finite or infinite?

Examples 1 and 2 use an explicit notation. Example 3 uses natural language. Example 4 and 6 use set builder notation.

Membership

If an element a belongs to a set A, write $a \in A$. Otherwise, $a \notin A$.

Example 1. $A_1 = \{1, 2, 3, ..., 75\}$ Does $2 \in A_1$? Does $-45 \in A_1$?

Example 2. $A_2 = \{m^2 + 1 : m \in \mathbb{Z}\}$

1. Does $2 \in A_2$?
2. $65 \in A_2$?
3. $-17 \in A_2$?
4. $49 \in A_2$?

Would any of the answers be different if $m \in \mathbb{R}$?

Subset

Definition. A set A is a *subset* of B if every element in A is also in B. We write $A \subseteq B$.

Example 1. $\{1, 3, 4, 5\} \subseteq \{1, 3, 4, 5\}$

Example 2. Is it true that $\mathbb{N} \subseteq \mathbb{Z}$? What about $\mathbb{R} \subseteq \mathbb{Z}$? Why or why not?

Definition. A set A is a *proper subset* of B if every element in A is also in B AND $A \neq B$. We write $A \subset B$.

Example 1. $\{1, 3, 5\} \subset \{1, 3, 4, 5\}$. Would $\subseteq$ also be correct?

Example 2. Does $A \subseteq B$ imply $A \subset B$? What about the other way? Can you find examples or sketch a proof?

Empty Set

Definition. The empty set denoted as $\varnothing, \emptyset, \{\}$ is the set that does not contain any elements. It is NOT nothing!

Example 1. $\{n : n \geq 0 \ \ \& \ \ n < 0\}$.

Example 2. $\{n : n \in \mathbb{Z} \ \ \& \ \ n^2 = -1\}$

Example 3. True or False: The empty set is a subset of any set.

Universal set

Definition. The universal set denoted U is the set that contains ALL elements (in the context of the problem). The universal set is usually defined at the beginning or implied.

> **Example 1.** If $S = \{2k : k \in \mathbb{Z}\}$ then an appropriate universal set would be $U = \mathbb{Z}$.

Power sets

Definition. Given a set S, its power set 2^S or $\mathcal{P}(S)$ is the set of ALL subsets of S. This means that all the elements in 2^S are sets.

Example 1. What is the power set of $\{a, b, c\}$?

Example 2. What is the power set of $\emptyset$?

Example 3. Give an example of a set S for which $\mathcal{P}(S) = S$?

Cardinality

Definition. The cardinality of S denoted $|S|$ is the number of elements in the set S.

Example 1. For $S = \{1, 2, 3, 4\}$, $|S| = 4$.

Example 2. Given $S = \{1, 2, \{1, 2, \emptyset, \{\emptyset\}\}, 4\}$, what is $|S|$?

Example 3. If S is *finite*, what is $|2^S|$? That is for any finite set, what is the size of its power set?

If a set is *infinite*, it is either countably infinite or uncountably infinite.

Set operations - Union

Definition. Let A and B be two sets. The **union** of A and B is defined as $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

Example 1. $A = \{1, 2, 3\}$ $B = \{2, 3, 4\}$. What is $A \cup B$?

Example 2. If U is the universal set and S is some other set, what is $U \cup S$?

Set operations - Intersection

Definition. Let A and B be sets. The **intersection** of A and B is defined as $A \cap B = \{x : x \in A \ \& \ x \in B\}$.

Example 1. $A = \{1, 2, 3\}$ $B = \{2, 3, 5, 6\}$. What is $A \cap B$?

Example 2. If U is the universal set. What is $\emptyset \cap U$?

Set operations - Complement

Definition. Let A be a set. The **complement** of A is defined using U as $\overline{A} = \{x : x \notin A \ \& \ x \in U\}$. (It is everything **not** in A).

Example 1. $A = \{1, 2, 3\}$. What is $\overline{A}$. Yes, this is a trick question.

Example 2. $A = \{1, 2, 3\}$ $U = \{x : 1 \leq x \leq 10, x \in \mathbb{Z}\}$. What is $\overline{A}$?

Example 3. What is $\overline{\emptyset}$ and $\overline{U}$?

Set operations - Difference

Definition. Let A and B be sets. The **difference** of A and B is defined as $A - B = \{x : x \in A \ \& \ x \notin B\}$. (Everything in A **not in** B).

Example 1. $A = \{1, 2, 3, 4, 5\}$ $B = \{2, 5, 6, 7\}$. What is $A - B$? $B - A$?

Example 2. What is $A - \emptyset$? $\emptyset - A$? $P(\emptyset) - \emptyset$?

Example 3. Rewrite $A - B$ using only the union ($\cup$), intersection ($\cap$) and complement ($-$) operator.

Set operations - Cross-product

Definition. The **cross-product** of A and B is defined as $A \times B = \{(a, b) : a \in A \ \& \ b \in B\}$. It is a set of two-tuples.

Example 1. $A = \{1, 2, 3\}$ $B = \{5, 6\}$. What is $A \times B$?

Example 2. What is $|A \times B|$?

Example 3. What is $S \times \emptyset$?

Set operations - Exercises

Let $U = \{1, 2, 4, 7, 8, 9, 10, 11\}, A = \{7, 8, 9\}, B = \{4, 9, 10\}$. What do the following set operations yield?

- **a.** $A \cup B = ...$
- **b.** $A \cap B = ...$
- **c.** $A - B = ...$
- **d.** $\overline{A} \cap B = ...$
- **e.** $A \times \{1, 2\} = ...$
- **f.** $(A \times B) \cap \emptyset = ...$
- **g.** $(\overline{A} \cup \overline{B}) \cup U = ...$
- **h.** $U \times \emptyset = ...$
- **i.** $(\overline{A} \cup \overline{\emptyset}) \cap U = ...$

Set operations - Some more properties

Given the set S, the following are always true:

1. $S \cup U = U$
2. $S \cap U = S$
3. $S \cup \emptyset = S$
4. $S \cap \emptyset = \emptyset$
5. $S \times \emptyset = \emptyset$
6. $\overline{\overline{S}} = S$
7. $\overline{\emptyset} = U$
8. $\overline{U} = \emptyset$

Theorem (De Morgan's Law). Given two sets S_1 and S_2:

$$\overline{S_1 \cap S_2} = \overline{S_1} \cup \overline{S_2}$$
$$\overline{S_1 \cup S_2} = \overline{S_1} \cap \overline{S_2}$$

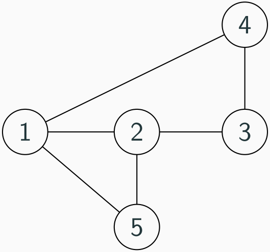
Review of graph theory

Definition of a graph

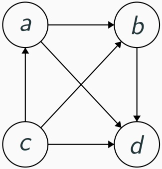
Definition. An **undirected graph** is a collection of points (called **vertices/nodes**) with lines (called **edges**) connecting some of the points.

In an undirected graph, there is no direction to the edges. In a directed graph, edges have have arrows to signal direction.

Example. The following are two examples of graphs. G_a is undirected, G_b is directed.



Graph G_a



Graph G_b

Formal representation of a graph

A graph can be represented pictorially or more formally by a set of vertices V and edges E.

For **undirected graphs**, we write $G = (V, E)$ where V is the set of vertices (more specifically their labels) and E is the set of edges where an edge is itself represented as a set $\{a, b\}$ of vertices.

For **directed graphs**, the notation is the same except that edges are represented by tuples (a, b) to signal that the edge goes out of a into b.

Example. The graphs from the previous slide could have also been written as

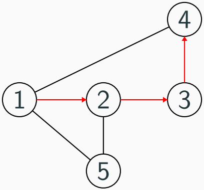
$$G_a = (\{1, 2, 3, 4, 5\}, \{\{1, 4\}, \{1, 2\}, \{1, 5\}, \{2, 5\}, \{2, 3\}, \{3, 4\}\})$$
$$G_b = (\{a, b, c, d\}, \{(a, b), (a, d), (b, d), (c, a), (c, b), (c, d)\})$$

Ways of "walking" through a graph

There are several different ways to "walk" through a graph. Each way has its own name and characteristics.

> A **walk** from vertex v_{i_1} to v_{i_n} is a sequence of edges $(v_{i_1}, v_{i_2}), (v_{i_2}, v_{i_3}), \ldots, (v_{i_{n-1}}, v_{i_n})$ where both vertices and edges may repeat. Notice that the sequence must be "contiguous" i.e. the edge e_i in the sequence must start at the destination vertex of e_{i-1}.
>
> A **path** is a walk in which no edge is repeated.
>
> A **simple path** is a path in which no vertex is repeated.

Example. (Simple) Path $(1, 2), (2, 3), (3, 4)$

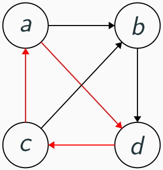


Ways of "looping" through a graph

There are also different ways to "loop" through a graph i.e. starting and ending at the same vertex.

- A **self-loop** or just **loop** is an edge that starts and ends at the same vertex. That is, its **outgoing** and **incoming** vertices are the same.
- A **circuit** with base v_i is a walk that starts and ends at v_i.
- A **cycle** is a circuit with no repeated edges.
- A **simple cycle** is a cycle with no repeated vertices other than its first vertex.

Example. (Simple) Cycle with base a, $(a, d), (d, c), (c, a)$



Trees!

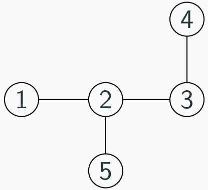
Definition. A graph $G = (V, E)$ is **connected** if for every pair of vertices $u, v \in V$ there is a path from u to v.

Definition. A **tree** is a connected acyclic graph. That is a connected graph with no cycles in it.

Definition. A **forest** is a (not necessarily connected) acyclic graph. A forest is usually thought of as a collected of unconnected trees.

Definition. A **rooted tree** is a directed tree that has one special vertex called the **root**. For every other vertex in the tree there exists a unique directed path to it from the root.

Example. Removing edges $\{1, 4\}$ and $\{1, 5\}$ from graph G_a makes it a tree



Review of (some) proof techniques

Equality of sets

Proof Technique. To prove for two sets A, B that $A = B$, one way of doing this is by "double inclusion" where you first show that $A \subseteq B$ and then $B \subseteq A$. To show that $A \subseteq B$, you must pick an arbitrary element $a \in A$ (i.e. an element for which you only know about its belonging to A) and show that it is is B.

Example

Example. Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Pigeonhole Principle

Proof Technique. The Pigeonhole Principle states that if there are $n+1$ pigeons occupying n holes, there must be a hole with two pigeons.

Example

Example. Let $G = (V, E)$ be a simple graph, if $|V| \geq 2$ there exists two vertices $u, v \in V$ with the same degree.

Proof by contradiction

Proof Technique. In a proof by contradiction, you assume that the premise of the statement you're trying to prove is false i.e. in if P then Q assume P is false. You then reason through a sequence of steps to arrive to a contradiction which may be 1. a refutation of what you initially assumed or 2. a refutation of something you know/have proved to be true.

Example

Example. If $T = (V, E)$ is a tree, then for any two vertices $u, v \in V$ there exists a unique path between them.

Proof by induction

Proof Technique. In a proof by induction, you want to prove a statement, $P(n)$, that depends on some integer n. For example, $P(n)$: "For $n \geq 5$, $2^n \geq n^2$". To do so, you must reason sequentially as follow

1. Prove the **base case (BC)** $\rightarrow$ show that $P(n)$ is true for the smallest possible value of n.
2. Assume the **inductive hypothesis** $\rightarrow$ assume that $P(n)$ is true for some arbitrary n.
3. Prove the **inductive step** $\rightarrow$ show that $P(n+1)$ is true.

Example

Example. Let $T = (V, E)$ be a tree. Prove that $|E| = |V| - 1$.

Proof by construction

Proof Technique. In statements that claim the existence of some property or object, one common approach is to construct this property or object in the proof. This proof technique will be <u>very common</u> in automata theory as you will see shortly.

Example

Example. (Sipser 0.10) For each even number n greater than 2, there exists a 3-regular graph with n vertices.