FOCS Notes
Lecture
1/17/2020

Agenda

- Discrete Objects
  - Sets
  - Sequences
  - Graphs
- Proof
  - In 4 rounds of the speed-dating app, no one meets more than 12 people
  - x^2 is even "is the same" as x is even
    - "if and only if"
    - "iff"
    - $\iff$
  - Among any 6 people is a 3-clique or a 3-war
  - Axioms: The well-ordering principle
  - $\sqrt{2}$ is not rational (is irrational)

Set: a collection of objects

- order and repetition don't matter
- $\mathbb{N} = \{1, 2, 3, \ldots\}$ (fact, "..." is ambiguous/lazy)
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \{0, \pm 1, \pm 2, \ldots\}$
  - $= \{0, -1, 1, 2, -2, 5, -5, 4, -4, \ldots\}$
  - $= \{0, 0, 1, 1, 2, 2, 2, -2, 3, -3, \ldots\}$
- $\mathbb{Q} = rational\ numbers = \{\pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{4}, \ldots, \pm\frac{2}{3}, \pm\frac{2}{5}, \ldots\}$
- $let\ \mathbb{P} = all\ valid\ computer\ programs$
- $let\ \mathbb{P}_{c++} = all\ valid\ c++\ listings$
- $let\ \mathbb{S} = \{a, 4, Alex\}$
- $let\ \mathbb{L} = valid\ literals\ in\ Python = \{"a", 'a', 4, 0x14, [1, 2], \{'x' : 2\}\}$
- Sets can contain other sets
  - $let\ \mathbb{S} = classes\ taught\ at\ RPI\ in\ Spring$ 2020 (where each class is the set of students in that class)
- Dealing with ambiguity of "..."
  - Ex: $\{1, 2, 3, \ldots\}$ could be $\mathbb{N}$ or positive primes
  - Solution: express the set with set builder notation (in terms of a variable and clause(s) that variable must satisfy)
  - $\{k | k\ is\ a\ natural\ number\} = \mathbb{N} = \{1, 2, 3, \ldots\}$
  - $\{k | k\ is\ a\ prime\} = \{1, 2, 3, \ldots\} = \{k | if\ a \in \mathbb{N}\ and\ a\ divides\ k,\ then\ a = 1\ or\ a = k\}$
  - $\mathbb{Q} = \{x | x = \frac{a}{b}; a \in \mathbb{N}\ and\ b \in \mathbb{N}\}$
  - $let\ \mathbb{P}_{c++} = \{x | gcc\ x\ runs\ without\ an\ error\ message\}$

Set operations

- $A \cap B = \{x | x \in A \ and \ x \in B\} \ \leftarrow$ "Intersect"
- $A \cup B = \{x | x \in A \ or \ x \in B\} \ \leftarrow$ "Union"
- $\bar{A} = \{x | x \notin A\} = A^c \ \leftarrow$ "Complement"
- We need to define a universal set in which all the relevant elements exist in order to have well-defined set operations
  - e.g. if $A = FOCS \ class$, then does $\bar{A}$ contain Barrack Obama?
  - Usually the universal set is obvious, but not always
- Set differences
  - $A - B = x | x \in A \ and \ x \notin B = A \cap \bar{B}$
- Similarly:
  - $\bigcup_{i=1}^{k} A_i = \{x | \exists i \in \{1, \ldots, k\} \ for \ which \ x \in A_i\}$
  - $\bigcap_{i=1}^{k} A_i = \{x | \forall i \in \{1, \ldots, k\}, x \in A_i\}$

Calculus of set operations

- $A \bar{\cup} B = \bar{A} \cap \bar{B}$
- $A \bar{\cap} B = \bar{A} \cup \bar{B}$
- $\bar{\bar{A}} = A$
- Ex: $A \bar{-} B = A \bar{\cap} \bar{B} = \bar{A} \cup B$

Set containment

- $A \subseteq B \iff x \in A \ means \ x \in B$
- $A \subset B \iff A \subseteq B \ and \ B \nsubseteq A$
  - $human \subseteq mammals \subseteq animals \ and \ mammals \nsubseteq humans \ and \ humans \subset mammals$

Sequence: a list of objects

- $aabcd \neq abcd \neq bacd$
- order and repetition matters
  - ex: binary strings like 00110111100

Graph

- useful for encoding relationships between elements
- $G = (V, E) \ \leftarrow$ graph is a tuple of vertices and edges
- $E = \{x | x = (u, v) \ for \ elements \ u, v \in V\}$
- Ex:
  - Gittens, Magdon-Ismail, Xu, Bennet, Goldschmidt, McGuinness, Weissman, Stevenson $\leftarrow$ vertices
  - Edges: every combination of McGuiness, Gittens, Magdon-Ismail, and Goldschmidt; combinations of Xu, Stevenson, and Bennet;

- $V = \{Gittens, Magdon - Ismail, \dots\}$
- $E = \{(Xu, Bennet), (Xu, Stevenson), \dots\}$

Proofs: a convincing argument of the truth of a claim (in this class mathematically convincing)

- Deductive reasoning: start off with agreed upon mathematical truths and derive claims that are true as their consequences
  - Ex: speed-dating will expose each person to at most 12 potential partners
    - Fact: in each round, a person will be exposed to at most 3 people
    - Fact: there are 4 rounds of dating
    - Consequence: I am exposed to at most 12 people
  - Claim: Every even square is the squar of an even number and every even number's square is even
  - Proof even number $\rightarrow$ even square
    - let k be an even number, $k = 2n$
    - this implies $k^2 = 4n^2 = 2(2n^2)$, so k^2 is even
  - Proof even square $\rightarrow$ it is the square of an even number
    - let k be an even square. Assume it is not the square of an even number, that is $k = (2n+1)^2 = 4n^2 + 2n + 1 = 2(2n^2 + n) + 1$
    - this says k is odd. Since k is even, this contradiction implies our assumption that k can be written as the square of an odd number is false
    - That is, k is the square of an even number
  - We can't prove everything
    - Axioms: claims we all agree to accept as true, "self-evident" truths
    - Conjecture: a claim that is believed to be true, but may not yet be proven
    - Theorem: a proven truth (unlike and axiom)
    - Axiom 1: well-ordering principle (for $\mathbb{N}$)
      - any non-empty set of positive integers has a smallest element
  - Proof: $\sqrt{2}$ is irrational (proof by contradiction aka *reductio ad absurdum*)
    - assume $\sqrt{2}$ is rational
    - then we can write $\sqrt{2}$ as $\{\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}, \dots\}$ for some set of rational numbers
    - consider the set of denominators $\{b_1, \dots\} \subset \mathbb{N}$
    - by the well-ordering principle for $\mathbb{N}$, this set has a smallest element, called b_*
    - we write $\sqrt{2} = \frac{a_*}{b_*}$
    - this implies $2 = \frac{a_*^2}{b_*^2} \;\rightarrow\; 2b_*^2 = a_*^2$
    - because a_*^2 is an even square, we know that a_* is even, $a_* = 2\bar{a}$
    - this implies $2b_*^2 = a_*^2 = 4\bar{a}^2 \;\rightarrow\; b_*^2 = 2\bar{a}^2$
    - because b_*^2 is an even square, we know b_* is even, $b_* = 2\bar{b}$
    - we now know that $\sqrt{2} = \frac{a_*}{b_*} = \frac{2\bar{a}}{2\bar{b}} = \frac{\bar{a}}{\bar{b}}$
    - i.e. we constructed a rational expression for $\sqrt{2}$ that has a smaller denominator than b_*. This contradicts the minimality of b_* that is guaranteed by the well-ordering principle
    - therefore $\sqrt{2}$ is not rational