Lecture 0' - Sets, Functions, Relations...

Vaishnavi Sundararajan

COL703 - Logic for Computer Science

1 Sets

All set?

- "Set" used to be the English word with the most definitions
- A mathematical set is a very simple concept that contains multitudes
- What is a set? A set is often defined as just "a collection of distinct things"
- What things? Animals? People? Other sets? **Just about anything!**
- $\{1, 2, 3, 4\}$ is a set
- $\{\text{Alice}, \text{Flamingos}, \text{Hedgehogs}, \text{Playing cards}, \text{Cheshire cat}\}$ is also a set!

More about sets

- $\{e4\ e5, e4\ c5, d4\ d5, c4\ e5, c4\ c5\}$ is also a set

More about sets

- $\{e4\ e5, e4\ c5, d4\ d5, c4\ e5, c4\ c5\}$ is also a set
- What is it a set of? Can we draw any inference about an element based on membership in this set?

More about sets

- $\{e4\ e5, e4\ c5, d4\ d5, c4\ e5, c4\ c5\}$ is also a set
- What is it a set of? Can we draw any inference about an element based on membership in this set?
- Could just be <letter><digit><space><letter><digit> sequences

More about sets

- $\{e4\ e5, e4\ c5, d4\ d5, c4\ e5, c4\ c5\}$ is also a set
- What is it a set of? Can we draw any inference about an element based on membership in this set?
- Could just be <letter><digit><space><letter><digit> sequences
- Or opening moves for famous chess openings

More about sets

- $\{e4\ e5, e4\ c5, d4\ d5, c4\ e5, c4\ c5\}$ is also a set
- What is it a set of? Can we draw any inference about an element based on membership in this set?
- Could just be <letter><digit><space><letter><digit> sequences
- Or opening moves for famous chess openings
- Helpful to give more information than just listing elements explicitly

More about sets

- $\{e4\ e5, e4\ c5, d4\ d5, c4\ e5, c4\ c5\}$ is also a set
- What is it a set of? Can we draw any inference about an element based on membership in this set?
- Could just be <letter><digit><space><letter><digit> sequences
- Or opening moves for famous chess openings
- Helpful to give more information than just listing elements explicitly
- State the property all set elements have in common!

More about sets

- $\{e4\ e5, e4\ c5, d4\ d5, c4\ e5, c4\ c5\}$ is also a set
- What is it a set of? Can we draw any inference about an element based on membership in this set?
- Could just be <letter><digit><space><letter><digit> sequences
- Or opening moves for famous chess openings
- Helpful to give more information than just listing elements explicitly
- State the property all set elements have in common!
- **Set builder notation**: Write a set as $\{x \mid 0 < x \leqslant 5 \text{ and } x \in \mathbb{N}\}$

Some important sets

- $\mathbb{U}$: The *universal* set (every element we want to talk about is in here)
- $\{\}$: The *empty* set (no element belongs to this set; often written as $\varnothing$)
- $\mathbb{Z}$: The set of all *integers* (both positive and negative)
- $\mathbb{N}$: The set of all *natural* numbers (every integer $\geqslant 0$)
- $\mathbb{Q}$: The set of all *rational* numbers (expressed as p/q for some $p, q \in \mathbb{Z}$)
- $\mathbb{R}$: The set of all *real* numbers
- $\mathbb{B} = \{\text{True}, \text{False}\}$: The set of Boolean values

Set membership

- Denote by $x \in S$ the fact that x is an element of the set S (negation: $x \notin S$)
- Each element occurs only once in a set (*distinct* elements!)
  - We take multiplicity into account for **multisets**
  - $\{1\}$ is a set consisting of the singleton element 1
  - $\{1, 1, 1\}$ is a multiset consisting of the element 1 appearing thrice
- **Set Equality**: Sets S_1 and S_2 are defined to be equal (denoted $S_1 = S_2$) if, for every element x, it is the case that $x \in S_1$ **if and only if** $x \in S_2$.
  - Reflexive, symmetric, and transitive congruence

Subset operation

- A is a subset of B (denoted $A \subseteq B$) if, for every element x of A, the element x also appears in B
- An element of a set might itself be a set
- A subset of a set **must** be a set
- $\text{Chars} = \{\text{Tintin}, \text{Haddock}, \text{Calculus}, \text{Snowy}, \{\text{Thomson \& Thompson}\}\}$
- $\{\text{Thomson \& Thompson}\} \in \text{Chars}$
- $\{\text{Tintin}, \text{Snowy}\} \subseteq \text{Chars}$
- The **powerset** of a set S (denoted 2^S) is the set of all subsets of S
- **Exercise**: For any set S, show that $S \subseteq \mathbb{U}$, as well as that $\emptyset \subseteq S$.

Union and Intersection

- **Union**: $S_1 \cup S_2 = \{x \mid x \in S_1 \textbf{ or } x \in S_2\}$
- **Intersection**: $S_1 \cap S_2 = \{x \mid x \in S_1 \textbf{ and } x \in S_2\}$
- Commutativity†: $S_1 \circ S_2 = S_2 \circ S_1$
- Associativity†: $S_1 \circ (S_2 \circ S_3) = (S_1 \circ S_2) \circ S_3$
- Idempotence†: $S \circ S = S$
- **Duality** between union and intersection
  - $\varnothing$ is an *identity* for union and an *annihilator* for intersection
  - $\mathbb{U}$ is an *identity* for intersection and an *annihilator* for union
- **Distributivity for union and intersection**:
  - $S_1 \cup (S_2 \cap S_3) = (S_1 \cup S_2) \cap (S_1 \cup S_3)$
  - $S_1 \cap (S_2 \cup S_3) = (S_1 \cap S_2) \cup (S_1 \cap S_3)$

†: $\circ$ can be union or intersection

Difference, Complement, and Cartesian product

- **Difference**: $S_1 \setminus S_2 = \{x \mid x \in S_1$ **and** $x \notin S_2\}$
- **Complement**: $\overline{S} = \mathbb{U} \setminus S$
- **De Morgan's Laws**: $\overline{S_1 \cup S_2} = \overline{S_1} \cap \overline{S_2}$ and $\overline{S_1 \cap S_2} = \overline{S_1} \cup \overline{S_2}$
- $S \cup \overline{S} = \mathbb{U}$ and $S \cap \overline{S} = \varnothing$, and $\overline{\mathbb{U}} = \varnothing$ and $\overline{\varnothing} = \mathbb{U}$
- **Exercise**: Show that $S_1 \setminus S_2 = S_1 \cap \overline{S_2}$
- **Cartesian product**: $S_1 \times S_2 = \left\{(x,y) \mid x \in S_1 \text{ and } y \in S_2\right\}$
- $S \times \varnothing = \varnothing \times S = \varnothing$
- Is the Cartesian product associative?
- $S_1 \times S_2 \times \ldots S_n = \left\{(s_1, s_2, \ldots, s_n) \mid s_i \in S_i \text{ for each } i\right\}$

Cardinality

- The number of elements in a set S is called its **cardinality**
- We denote the cardinality of a set S by $|S|$
- $S = \{0, 1, 2, 3, 4, 5\}$ is a finite set
- The set of real values in the interval $[0, 1]$ is infinite
- Sets can be one or more of
  - Bounded
  - Finite
  - Unbounded
  - Infinite
- Do any of these necessarily imply any others?
- Are there combinations which are not possible?

Infinite sets

- Not all infinite sets are equally infinite!
- Infinite sets can be **countable** or **uncountable**
- What does it mean to be countable?
- "One can uniquely associate each element with a natural number"
- How does one formally capture such an association? Via **functions**
- But first, we will talk about **relations**

Relations

- A **binary relation** R between two sets A and B is any subset of $A \times B$
- We will often write xRy to denote that $(x, y) \in R$
- $\text{dom}(R) = \{a \in A \mid aRb \text{ for some } b \in B\}$
- $\text{rng}(R) = \{b \in B \mid aRb \text{ for some } a \in A\}$
- $R \subseteq A \times B$ is
    - *total* if for each $x \in A$, there is a $y \in B$ such that xRy
    - *one-one* if xRy and zRy implies $x = z$ (any $y \in B$ related to at most one $x \in A$)
    - *onto* if for each $y \in B$, there is an $x \in A$ such that xRy
- $R \subseteq A \times B$ a graph with edges from elements of A to elements of B

More about relations

- **Identity relation**: $\mathrm{id}(S) = \{(x, x) \mid x \in S\}$
- **Relational composition**: If $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$, then the relational composition of R_1 and R_2 (denoted $R_1 \circ R_2$) is: $R_1 \circ R_2 = \{(a, c) \mid \text{There is some } b \in R \text{ such that } (a, b) \in R_1 \text{ and } (b, c) \in R_2\}$
- For any $R \subseteq A \times B$, we have $\mathrm{id}(A) \circ R = R = R \circ \mathrm{id}(B)$
- **Exercise**: For binary relations $R_1, R_1' \subseteq A \times B$ and $R_2, R_2' \subseteq B \times C$ with $R_1 \subseteq R_1'$ and $R_2 \subseteq R_2'$, show that $R_1 \circ R_2 \subseteq R_1' \circ R_2'$.

More about relations

- **Relational inverse**: For $R \subseteq A \times B$, the *inverse* of R is defined as $R^{-} = \left\{(y, x) \mid xRy\right\}$
- For every set S, $(\mathrm{id}(S))^{-} = \mathrm{id}(S)$, and for every relation R, $(R^{-})^{-} = R$
- **Exercise**: Show that for any relations R_1 and R_2, $(R_1 \circ R_2)^{-} = (R_2)^{-} \circ (R_1)^{-}$
- Reflexivity: $R \subseteq S \times S$ is *reflexive* if xRx for every $x \in S$.
- Symmetry: $R \subseteq S \times S$ is *symmetric* if xRy implies yRx.
- Transitivity: $R \subseteq S \times S$ is *transitive* if xRy and yRz implies xRz.
- *Equivalence relation*: Reflexive, symmetric, and transitive
- R is *functional* (i.e. corresponding to a **function**) if xRy and xRz implies $y = z$ (any $x \in A$ related to at most one $y \in B$)

Functions

- Consider a functional relation $R_f \subseteq A \times B$.
- We write $f : A \longrightarrow B$ and $f(x) = y$ whenever $(x, y) \in R_f$ (often denoted $x \longmapsto y$)
- A is the pre-domain of f and B is the co-domain of f
- R_f is the graph of f
- $\mathrm{dom}(f)$ and $\mathrm{rng}(f)$ defined as for R_f
- We call f a *total/one-one/onto* function if R_f is total/one-one/onto
- f is called a **bijection** if it is both one-one and onto
- For a bijective f, there exists a natural inverse f^{-1} (whose graph is R_f^-)
- Sets A and B are said to be *in bijection* with each other if there is a bijection f such that $f : A \longrightarrow B$.

Back to infinite sets

- A set S is *countable* if there is a function f which maps $\mathbb{N}$ **onto** S
- Can use $\mathbb{N}$ to "uniquely count" the elements of S
- $\mathbb{N}$ is countable (obviously!)
- **Exercise**: Show that the set of odd natural numbers is countable, and has cardinality *equal* to that of $\mathbb{N}$.
- **Exercise**: Show that $\mathbb{N} \times \mathbb{N}$ is countable.
- The countable union of countable sets remains countable.

More infinite sets

- More {infinite sets}:
  - $\mathbb{Q}$ is countable
  - $\mathbb{Z}$ is countable
  - $A^n = \{(a_1, \ldots, a_n) \mid a_i \in A \text{ for each } i\}$ is countable
- {More infinite} sets:
  - The powerset of $\mathbb{N}$ is **uncountable**
  - $\mathbb{R}$ is uncountable: Shown by Georg Cantor using **diagonalization**
- Basically a proof by contradiction
- If any subset of a set is uncountable, then the set itself must be uncountable

Cantor's diagonal argument

- Assume $(0, 1)$ is countable.
- (Countable) set S of all non-terminating decimals in $(0, 1)$
  - Each real number has just one representation
  - Each rational has two – choose the one with infinitely many trailing 9s
- Some onto function $f : \mathbb{N} \to S$ exists
- Can put each element of S in its own row (element x goes into row i if $f(i) = x$)
- Each element of the form $0.d_{i0}d_{i1}\ldots$ for every i
- Put $r_i = d_{i0}d_{i1}\ldots$ in the i^{th} row

Cantor's diagonal argument (contd.)

- Consider a non-terminating decimal $r = u_0 u_1 \dots$ s.t. $u_i \neq d_{ii}$.

$$\text{For example, } u_i = \begin{cases} d_{ii} + 1, & \text{if } d_{ii} < 9 \\ d_{ii} - 1, & \text{otherwise} \end{cases}$$

- Essentially: choose an r such that the digit at the i^{th} position is different from that along the diagonal of our enumeration. $r \in S$.
- For every m there is already some r_m in the m^{th} row
- But the m^{th} digit of r was chosen to be different from d_{mm}, so $r \neq r_m$
- There is no $k \in \mathbb{N}$ s.t. $f(k) = r$, which contradicts the onto-ness of f!

Proving statements about infinite sets

- Prove statements about finite sets by (potentially painful) case analysis
- But what about infinite sets? Say I want to prove something about $\mathbb{N}$.
- Could test it for some naturals. Is this convincing?
- Suppose I set a computer to do this
- The computer runs out of memory/power at some point
- Infinitely many naturals, but we can only examine finitely many
- What if the counterexample to the claim lies outside of this subset?
- Need **induction**

(Weak) Mathematical induction

- Prove it for the “smallest” candidate.
- Then show that if the statement is true about one candidate, then it is also true about the “next” candidate.
- This process “runs forever” – we never run out of “next” candidates
- But a uniform template for every “next” candidate allows us to claim something about *all* candidates.
- Somewhat like a `while(true)`, without any of the nasty segfaults!
- One of Peano’s axioms for characterizing $\mathbb{N}$: Let $A \subseteq \mathbb{N}$. If $0 \in A$ and for every $x \in \mathbb{N}$, if $x \in A$ implies $x + 1 \in A$, then $A = \mathbb{N}$.

Other kinds of induction?

- **Variant of mathematical induction**: If a statement is true about **the "previous" candidate**, then it is also true about the current candidate.
- **Strong/Complete induction**: If a statement is true about **every candidate from the smallest through the current one**, then it is also true about the"next" candidate.
- Next time: **Structural induction**