Lecture 1 - Orderings & Induction

Vaishnavi Sundararajan

COL703 - Logic for Computer Science

Recap

- Sets, relations, functions
- One-one/onto functions
- Finite and infinite sets
- Differently infinite sets – diagonalization

1. Working with infinite sets
2. Order, order!
3. Induction: New and improved

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.

1. Working with infinite sets

2. Order, order!

3. Induction: New and improved

What “next”?

- We say “next”, “previous”, “smallest” etc
- How are we measuring this?
- Do I know that there is exactly one such?
- Can I still use induction if there are multiple “next”s or “smallest”s?
- First: “Smallest” according to what? Is there always a “the smallest”?

Orders

- For the naturals, we used the "less than" binary relation
- Convenient notion
  - Any two naturals linked via this (total) relation
  - Clear notion of a "next" (add one) and a "smallest" (zero)
- Antisymmetric (if $m < n$ then $n \not< m$ for any m, n)
- Transitive (if $m < n$ and $n < p$, then $m < p$)
- But not reflexive ($n \not< n$ for any n)
- A "better" relation to consider: $\leq$
  - This kind of relation occurs more frequently
  - More amenable to algebraic treatment
- Cycle back to $<$ when we talk about well-foundedness

Partial orders

- **Partial** order: relation that is reflexive, antisymmetric and transitive
- A partial order $\preccurlyeq$ over X defined as follows
  - $x \preccurlyeq x$ for every $x \in X$
  - If $x \preccurlyeq y$ and $y \preccurlyeq x$, then $x = y$ for any $x, y \in X$
  - If $x \preccurlyeq y$ and $y \preccurlyeq z$, then $x \preccurlyeq z$ for any $x, y, z \in X$
- $(X, \preccurlyeq)$ is a *partially-ordered set* (poset)
- *Partial* because there might be some $x, y \in X$ s.t. $x \not\preccurlyeq y$ **and** $y \not\preccurlyeq x$

Examples of orders

- $\leq$ on $\mathbb{N}$ (total)
- Lexicographic ordering on words in a language (total)
- "Can fit" relation (with direction) on jigsaw pieces (partial)
- $\subseteq$ on the powerset of any set X (partial)
- Ancestry relation on the set of nodes in a tree (partial)
- Substring ordering on words in a language (partial)

Properties of posets

- A poset $(X, \preccurlyeq)$ could have minimum and maximum elements
    - Minimum element a: for every $x \in X$, $a \preccurlyeq x$
- If a poset $(X, \preccurlyeq)$ has a minimum element, it has exactly one.
    - Suppose two elements a and a' are both minimum for $(X, \preccurlyeq)$
    - a is minimum: $a \preccurlyeq a'$
    - a' is minimum: $a' \preccurlyeq a$
    - By antisymmetry, $a = a'$
- Maximum element b: for every $x \in X$, $x \preccurlyeq b$
- If a poset $(X, \preccurlyeq)$ has a maximum element, it has exactly one.

Minimum vs minimal

- Minimal element a for $(X, \preccurlyeq)$: for every $x \in X$, if $x \preccurlyeq a$, then $x = a$.
- Maximal element b for $(X, \preccurlyeq)$: for every $x \in X$, if $b \preccurlyeq x$, then $x = b$.
- For $(X, \preccurlyeq)$, if a is minimum, then it is also minimal
- But the converse is not necessarily true! (Why?)
- If $\preccurlyeq$ is a total order on X, then minimal implies minimum.
- Similarly for maximum vs maximal.
- It is possible for a poset to **not** have any subset of {minimum, minimal, maximum, maximal} elements.

More about posets

- $a \in X$ is said to be a *lower bound* of $S \subseteq X$ iff $a \preccurlyeq x$ for every $x \in S$
- A subset S might have zero, one, or multiple lower bounds
- It could also be that none of the lower bounds exist inside S
- Examples?
- A notion of a *greatest lower bound*
- Similar notions of a *least upper bound*

Well-founded sets

- Irreflexive, antisymmetric, transitive relation $\prec$ on a set X
- Minimal element a: No $x \in X$ such that $x \prec a$
- $(X, \prec)$ is **well-founded** if every nonempty $S \subseteq X$ has a minimal element.
- Every well-founded set has at least one minimal element (Obviously!)
- **Thm:** $(X, \prec)$ is well-founded **iff** it has **no infinite descending chain**, i.e. $a_1 \succ a_2 \succ a_3 \succ \ldots$ (where each $a_i \in X$, and $\succ$ is the inverse of $\prec$)
- $(\Longrightarrow)$ Suppose there is an infinite descending chain, then that subset has no minimal element, contradicts the well-foundedness of $(X, \prec)$
- $(\Longleftarrow)$ Suppose $(X, \prec)$ is **not** well-founded, demonstrate a contradiction by constructing an infinite descending chain.

Well-founded induction

- Let $(X, \prec)$ be a well-founded set
- Let P be a statement about the elements of X
- Can state an induction principle for $(X, \prec)$ as follows
- If we can prove the following: "For every $x \in X$, if P holds for all $y \in X$ such that $y \prec x$, then P holds for x too"
- Then P holds for every $x \in X$
- Special case: Strong mathematical induction
  - Well-ordered set $(\mathbb{N}, <)$
  - All descending chains are finite (0 is the minimal element for $\mathbb{N}$ wrt $<$)
- Useful for proving properties about inductively-defined structures

Inductively-defined structures

- A nice way of building the set of natural numbers: **induction**
- Consider some large universe $\mathbb{U}$ of numbers. Now consider a set $X \subseteq \mathbb{U}$ such that • $0 \in X$, and • if $n \in X$, then $n + 1 \in X$.
- Define $\mathbb{N}$ to be the smallest such set X.

Inductively-defined structures

- Correspond neatly to recursive programs
- Need a base case, and an inductive step specified via functions
- Examples: The sets of all
  - **Natural numbers**: $n := 0 \mid n + 1$
  - **Lists***: $l :=$ Empty list $\mid$ Append $a\ l$
  - **Binary trees***: $T :=$ Empty tree $\mid$ Node $T\ n\ T$
  - **Words***: $w := \varepsilon \mid a.w$
- * indicates adherence to a typing discipline
- The set of all lists over a particular type, all words over a particular alphabet etc.

Towards a generalized induction principle

- Suppose we want to show that property P holds for all $n \in \mathbb{N}$
- P might hold for more things in $\mathbb{U}$ as well
- Let $P' = \{x \in U \mid P(x)\}$
- Enough to show that $\mathbb{N} \subseteq P'$, i.e.
  - $0 \in P'$
  - If $n \in P'$, then $n + 1 \in P'$
- Equivalent to: P holds of 0, and if P holds of n, then P holds of $n + 1$
- But this is just **mathematical induction**!
- Leads us to **structural induction**

Structural induction

- Suppose you inductively defined a set S as the smallest subset of a larger universe $\mathbb{U}$ such that
  - *Some (base) elements from* $\mathbb{U}$ belong to S, and
  - If some elements belong to S, then the result of *applying some function* f *to those elements also belongs to* S
- How does one show that all elements of S satisfy a property P?
  - P holds for all base elements, and
  - If P holds for $\{x_1, \ldots, x_n\} \subseteq \mathbb{U}$, then P holds for $f(x_1, \ldots, x_n)$ (where f, as above, is n-ary)
- Allows us to prove properties about more complex inductively-defined structures

Two specifications

- $\mathbb{N}$ was specified in *Backus-Naur Form* (BNF) $\quad n := 0 \mid n+1$
- Now define $\mathbb{N}$ as the countable union of sets $X_0, X_1, \ldots$ where each X_i is the subset of $\mathbb{U}$ which we throw in at step i.
- $X_0 = \{0\}$ and $X_{i+1} = X_i \cup \{i+1\}$ for every $i > 0$ $\quad \mathbb{N} = \bigcup_{i \geq 0} X_i$
- Can we show that these two specifications yield the same set?
- **Exercise**: Show that if k is generated via the BNF, then $k \in X_i$ for some i, and vice versa.