Discrete Mathematics

Yi Li

Software School
Fudan University

March 13, 2012

Review of Lattice

- Ideal
- Special Lattice
- Boolean Algebra

Examples of Proof

- Zeno's paradox
- Zhuang Zi's paradox
- Gong Sunlong's "a white horse is not a horse"
- ...

How can you **persuade** yourself and the others?

Examples of Proof

Axiom

The axiom of group theory can be formulated as follows:

(G1) *For all* x, y, z*:* $(x \circ y) \circ z = x \circ (y \circ z)$.

(G2) *For all* x*:* $x \circ e = x$.

(G3) *For every* x *there is a* y *such that* $x \circ y = e$.

Theorem

For every x *there is a* y *such that* $y \circ x = e$.

What is Logic

- Premise
- Argument
- Conclusion
- Follow
- Proof

History of Mathematical Logic

- Aristotle(384-322 B.C.): theory of syllogistic
- De Morgan(1806-71), Boole(1815-64), Schröder(1841-1902)
- Frege(1848-1925), Russell(1872-1970)
- Post(1897-1954), Gödel (1906-78), Henkin(??), Herbrand(1908-31)
- Robbinson(1930-); Beth and Smullyan
- Leibniz(1646-1716) and Hilbert(1862-1943)

Introduction to Mathematical Logic

- First order logic
  - Propositional Logic
  - Predicate Logic
- High order logic
- Other type of logic
  - Modal logic
  - Intuitionistic logic
  - Temporal logic

Introduction to Mathematical Logic

- Proof system
  - Axiom
  - Tableaux
  - Resolution
- Two Components
  - Syntax
  - Semantics
- Algorithmic approach

Order

Definition (Partial order)

A *partial order* is a set S with a binary relation $<$ on S, which is *transitive* and *irreflexive*.

Definition (Linear order)

A partial order $<$ is a *linear order*, if it satisfies the *trichotomy* law: $x < y$ or $x = y$ or $y < x$.

Definition (Well ordering)

A linear order is *well ordered* if every nonempty set A of S has a least element.

Countable and Infinite

Definition (Countable)

A set A is *countable* if there is a one-to-one mapping from A to $\mathcal{N}$.

Definition (Finite)

A set A is *finite* if there is a one-to-one mapping from A to $\{0, 1, \ldots, n-1\}$ for some $n \in \mathcal{N}$.

Definition

1. If A is not countable, it is *uncountable*.
2. If A is not finite, it is *infinite*.

Countable and Infinite

Theorem

Let A be a countable set. The set of all finite sequence of elements in A is also countable.

Proof.

We can formalize it as
$S = \cup_{n \in \mathcal{N}} A^n = A^1 \cup A^2 \cup \cdots \cup A^n \cup \cdots$.
Construct a mapping from A^n to $\mathcal{N}$. □

Trees

Definition (Tree)

A *tree* is a set T(whose elements are called nodes) partially ordered by $<_T$, with a unique least element called the *root*, in which the predecessors of every node are well ordered by $<_T$.

Definition (Path)

A *path* on a tree T is a maximal linearly ordered subset of T.

Tree

Definition (Properties of tree)

1. The *levels* of a tree T are defined by induction.
2. The 0^{th} level of T consists precisely of the root of T.
3. The $k+1^{th}$ level of T consists of the immediate successors of the nodes on the k^{th} level of T.

Tree

Definition (Properties of tree)

1. The *depth* of a tree T is the maximum n such that there is a node of level n in T.
2. If there are nodes of the level n for every natural number n, we say the depth of T is infinite of ω.

Tree

Definition (Properties of tree)

1. If each node has at most n immediate successors, the tree is n-*ary* or n-*branching*.
2. If each node has finitely many immediate successors, we say that the tree is *finitely branching*.
3. A node with no successors is called a *leaf* or a *terminal node*.

Tree

Theorem (König's lemma)

If a finitely branching tree T is infinite, it has an infinite path.

Proof.

1. If there is no infinite path, the tree would be finite.
2. Split the successors of the node into two parts. One with inifinite successors and the other with finite successors.

□

Tree

Definition

A *labeled tree* T is a tree T with a function (the labeling function) that associates some objects with every node. This object is called the *label* of the node.

Tree

Definition (Segment)

1. σ is an *initial segement* of τ if $\sigma \subset \tau$ or $\sigma = \tau$.
2. σ is an *proper initial segement* of τ if $\sigma \subset \tau$.

Definition (Lexicographic ordering)

For two sequences σ and τ we say that $\sigma <_L \tau$ if $\sigma \subset \tau$ or if $\sigma(n)$, the n^{th} entry in σ, is less than $\tau(n)$ where n is the first entry at which the sequences differ.

Tree

One way to define a linear order based on given tree.

Definition (left to righ ordering)

Given two nodes x and y,

1. If $x <_T y$, we say that $x <_L y$.
2. If x and y are incomparable in the tree ordering, find the largest predecessors of x and y, say x' and y'
    1. If x' equals y', $x \leq y$ if and only if x is left to y relative to x'.
    2. Otherwise $x <_L y$ if and only if $x' <_L y'$.

Next Class

- Language of proposition logic
- Formation tree
- Truth table
- Connectives