Lecture 09-10: Chapter 1 Review & Sets

Jingjin Yu | Computer Science @ Rutgers

October 02, 2020

Outline

- Lectures 07-08 review
- Chapter 1 review
  - Logic & proofs
  - Definitions, axioms, theorems
  - Propositional logic: syntax & semantics
  - Extension to predicate logic
  - Rules of inference
  - Informal proofs & proof strategies
- Sets [2.1-2.2]

- A repeating note: **make sure you read the textbook**

L07-08: What was Covered

- Exhaustive proofs
  - Exclusive enumeration
  - Non-exclusive cases
- Existence proofs
  - Providing an example
  - Proving existence without an example
- Uniqueness proof
- Strategies
  - Reasoning backwards
  - Adapting existing proofs
  - Finding counterexamples

L07-08: Exhaustive Proof

- **Ex**: You have a drawer filled with red or blue socks. Show that if you pick three socks, you will have a pair of socks of the same color.

- **Ex**: Show that $((x > 4) \vee (y > 2)) \rightarrow (|x| + y^2 > 4)$.

L07-08: Existence Proof

- **Ex:** Show that there are positive integers that can be written as the sum of cubes of integers in two different ways.

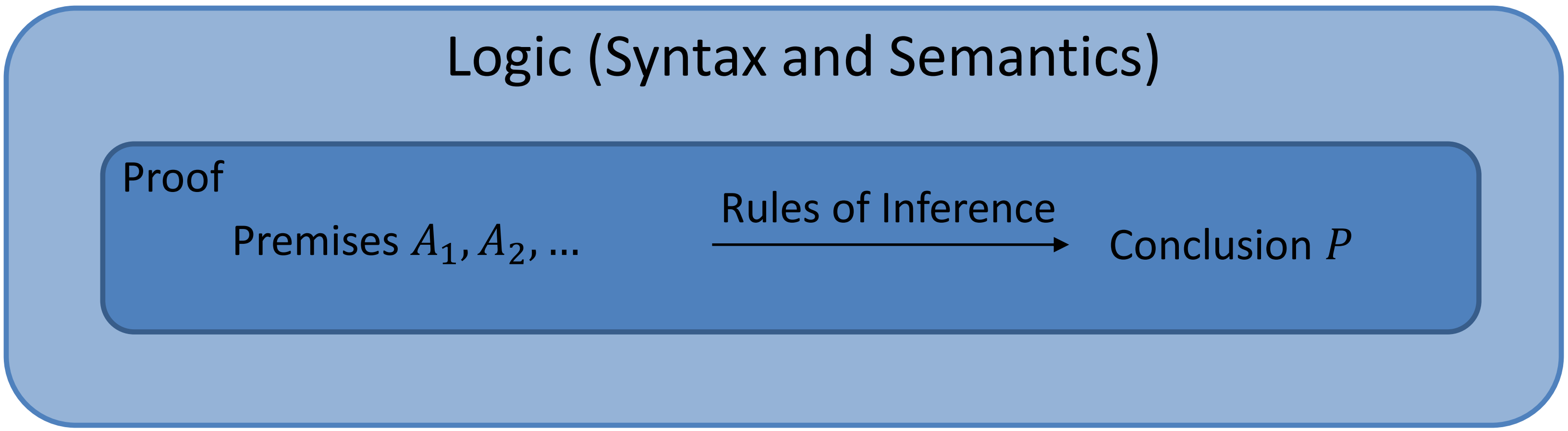
- **Ex:** Prove the existence of irrational numbers x and y such that x^y is rational.

L07-08: Uniqueness & Proof Strategies

- Uniqueness proofs: $\exists x\ (P(x) \wedge \forall y((y \neq x) \rightarrow \neg P(y)))$
- Strategies
  - Reasoning backwards: stone removal
  - Adapting existing proofs
    - **Ex:** Show that $\sqrt{3}$ is irrational.
    - (Generalization) If p is prime, then $\sqrt{p}$ is irrational.
    - (Further generalization) If n is not a perfect square, then $\sqrt{n}$ is irrational.

CH01: Logic and Proofs

- Whenever we talk about proofs, we need to specify a logic
  - Syntax: how to form sentences (definitions, axioms, propositions)
  - Semantics: how to interpret meaning and reason (with rules of inference)



- Chapter 1 covered:
  - Propositional logic
  - Predicate logic
  - Rules of inference, formal
  - Informal proofs, methods and strategies

CH01: Definitions, Axioms, Theorems

- We work mostly with definition and theorems
  - A definition defines what an entity is
  - A theorem relates different definitions
- Axiom: a proposition that is assumed to be true
- Theorems have many “variants”
  - Observation: an obvious (provable) statement
  - Theorem: a reasonably important result
  - Lemma: intermediate theorems for proving a concluding result
  - Proposition: a standalone, not very important theorem
  - Corollary: a derivative result that is worth stating and follows other theorems
    - Theorem: the sum of internal angles of a non-self-intersecting n-gon is $(n-2)*180$
    - Corollary: the sum of the internal angles of a triangle is 180.
      - A derivative but very useful result worth knowing

CH01: Propositional Logic: the Syntax

"can be" "or"

$$
\begin{array}{rcl}
Sentence & \rightarrow & AtomicSentence \mid ComplexSentence \\
AtomicSentence & \rightarrow & True \mid False \mid p \mid q \mid r \mid \ldots \\
ComplexSentence & \rightarrow & (\ Sentence\ ) \mid [\ Sentence\ ] \\
& \mid & \neg\ Sentence \\
& \mid & Sentence \land Sentence \\
& \mid & Sentence \lor Sentence \\
& \mid & Sentence \ \rightarrow\ Sentence \\
& \mid & Sentence \ \leftrightarrow\ Sentence
\end{array}
$$

"propositions"

- A sentence(proposition) can be an atomic sentence or a complex sentence
- E.g. $(p \lor q) \rightarrow (r \lor s)$
  - Propositions p, q, r, s are atomic sentences
  - $(p \lor q)$ is a complex sentence
  - So are $(r \lor s)$ and $(p \lor q) \rightarrow (r \lor s)$

- Truth table

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$	$\neg p \to \neg q$ (converse)	$q \to p$ (inverse)	$\neg q \to \neg p$ (contrapositive)
T	T	F	T	T	T	T	T	T	T
T	F	F	F	T	F	F	T	T	F
F	T	T	F	T	T	F	F	F	T
F	F	T	F	F	T	T	T	T	T

- A note on $p \to q$
  - Many equivalent statements

p implies q	q is **necessary** for p
If (when) p, (then) p	q follows p
p is sufficient for q	q if (when) p
p only if q	…

  - E.g., "You can graduate only if you have 150 credits"
    - If you graduated, then you must already have 150 credits
    - 150 credits is **necessary** for graduation (but may not be sufficient, e.g., maybe you decide to use the credit toward degree at another school)
    - Graduation **sufficiently** implies that you have at least 150 credits

CH01: Propositional Logic Semantics Cont.

Name	Equivalence
Identity laws	$p \wedge T \equiv p$, $p \vee F \equiv p$
Domination laws	$p \vee T \equiv T$, $p \wedge F \equiv F$
Idempotent laws	$p \vee p \equiv p$, $p \wedge p \equiv p$
Double negation law	$\neg(\neg p) \equiv p$
Commutative laws	$p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$
Associative laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Distributive laws	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
De Morgan's laws	$\neg(p \vee q) \equiv \neg p \wedge \neg q$, $\neg(p \wedge q) \equiv \neg p \vee \neg q$
Absorption laws	$p \vee (p \wedge q) \equiv p$, $p \wedge (p \vee q) \equiv p$
Negation laws	$p \vee \neg p \equiv T$, $p \wedge \neg p \equiv F$

Equivalence Containing Conditionals
$p \rightarrow q \equiv \neg p \vee q$
$p \rightarrow q \equiv \neg q \rightarrow \neg p$
$p \vee q \equiv \neg p \rightarrow q$
$p \wedge q \equiv \neg(p \rightarrow \neg q)$
$\neg(p \rightarrow q) \equiv p \wedge \neg q$
$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Equivalence Containing Bidirectionals
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

CH01: Extension to Predicate Logic

- Predicate: a property that objects may or may not satisfy
  - E.g. $StarTrekFan(x)$: whether student x is a Star Trek fan
  - Can be viewed as a partial proposition
  - Possible to have multiple variables: $Larger(x, y) = (x > y)$
- Quantifiers
  - Universal: $\forall x\ P(x)$, $P(x)$ is true for all x
  - Existential: $\exists x\ P(x)$, $P(x)$ is true for at least one x
  - Note that in general, $\exists x \forall y P(x, y) \neq \forall y \exists x P(x, y)$
- Binding: a variable is bound in a predicate when a quantifier of that variable is applied to the predicate, e.g. $\forall x \exists y\ (P(x, y) \vee Q(y))$
  - If all variables are bound, then the statement must be either true or false
- Negation: $\neg(\forall x P(x)) = \exists x(\neg P(x))$, $\neg(\exists x P(x)) = \forall x(\neg P(x))$.
  - Recursive application for multiple quantifiers
  - $\neg \forall x \exists y(P(x, y) \vee Q(y)) = \exists x \forall y(\neg P(x, y) \wedge \neg Q(y))$

CH01: Rules of Inference

- Propositional
  - Modus ponens

$$\begin{array}{l} p \to q \\ p \\ \hline q \end{array}$$

  - Modus tollens

$$\begin{array}{l} p \to q \\ \neg q \\ \hline \neg p \end{array}$$

Rule	Tautology	Name
$p \to q$ $q \to r$ $p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\neg p$ q	$((p \lor q) \land \neg p) \to q$	Disjunctive syllogism
p $p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ p	$(p \land q) \to p$	Simplification
p q $p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunction
$p \lor q$ $\neg p \lor r$ $q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	Resolution

- With quantifiers
  - Universal instantiation: $\forall x P(x) \to P(c)$ for any c
  - Existential instantiation: $\exists x P(x) \to P(c)$ for at least one c
  - Universal generalization: $P(c)$ for arbitrary $c \to \forall x P(x)$
  - Existential generalization: $P(c) \to \exists x P(x)$

CH01: 1.6 Exercise 28

- If $\forall x\big(P(x) \vee Q(x)\big)$ and $\forall x\Big(\big(\neg P(x) \wedge Q(x)\big) \rightarrow R(x)\Big)$ are true, then $\forall x(\neg R(x) \rightarrow P(x))$ is also true.

CH01: Informal Proofs

- How to approach proofs?
  - Requires creativity in general, but there are some rules to follow
  - First, pick how you will attack
    - Direct proof: prove $(p \to q) = T$ by assuming p=T and derive q=T
    - Proving contrapositive: prove $p \to q$ by proving $\neg q \to \neg p$
    - Proof via contradiction: to prove p=T, assume $\neg p$ and derive a contradiction
  - Next, examine the scope
    - Exhaustive proof must show $\forall x P(x)$
    - Existence proof only needs to establish $\exists x P(x)$
      - Can be constructive or non-constructive
    - Uniqueness proof requires showing $\exists ! x P(x)$
  - Then, try to get the details
    - Working from the start and/or from the goal – try to connect
    - Adapting or generalizing existing proofs
      - This means that one may look at some simple cases first

Sets

- $\mathbf{Def}^{n}$: A **set** is an unordered collection of objects (or elements, members).
- Membership: $a \in A, b \notin A$

- Roster representation
  - $\mathbf{Ex}$: The set of all vowels: $V = \{a, e, i, o, u\}$.
  - $\mathbf{Ex}$: The set of positive odd integers less than 10: $O = \{1,3,5,7,9\}$.
  - $\mathbf{Ex}$: Elements do not need to be of the same type: $A = \{1, 3.4, ball, tree\}$.
  - $\mathbf{Ex}$: The set of natural numbers: $N = \{0,1,2, \dots\}$.
    - A word about the number 0…

- Frequently seen sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Builder Notation, Equivalence, Empty Set

- Set builder notation: $A = \{x \mid \text{property satisfied by } x\}$
  - **Ex**: $O = \{x \mid (0 \leq x \leq 10) \wedge (x \text{ is odd})\}$.
  - **Ex**: Intervals on a line:
    - $(a, b) = \{x \mid a < x < b\}$
    - $(a, b] = \{x \mid a < x \leq b\}$
    - $[a, b) = \{x \mid a \leq x < b\}$
    - $[a, b] = \{x \mid a \leq x \leq b\}$
  - **Ex**: $A = \{x \mid x \text{ is a student at Rutgers}\}$

- **Def^n**: Two sets A and B are equal if they contains the same elements.
  - Equivalently, $A = B$ if and only if $\forall x(x \in A \leftrightarrow x \in B)$.

- The empty set: $\emptyset = \{\}$, the set that contains zero elements.
  - Note: $\{\emptyset\} \neq \emptyset = \{\}$
  - $\{\emptyset\}$ is a set with one element, which is the empty set (as an element)

Subsets

- **Def^n**: A is a subset ($\subseteq$) of B if every element of A is also an element of B.
- **Ex**: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
- **Ex**: $A = \{1, 3, 5, \ldots\}$, $A \subseteq \mathbb{N}$
- **Ex**: $A = \{CS\ 205\ students\}$, $B = \{Rutgers\ students\}$, $A \subseteq B$
- Equivalently, $A \subseteq B$ if and only if $\forall x(x \in A \rightarrow x \in B)$.
  - The symbols $\subset$ and $\subseteq$ generally bear the same meaning.
  - For **proper** subset, we generally use $A \subsetneq B$
    - **Ex**: $\mathbb{Z} \subsetneq \mathbb{R}$
    - Note that it is possible that $A \subsetneq B$ and $A \subseteq B$ both hold

- To prove $A \subseteq B$, can show $c \in A \rightarrow c \in B$ for arbitrary $c \in A$.
- To prove $A \subsetneq B$, show $A \subseteq B$ and there is a c s.t. $c \in B$ and $c \notin A$.
- To prove $A = B$, show $A \subseteq B$ and $B \subseteq A$.

- Fact: for every set S, $\emptyset \subseteq S$ and $S \subseteq S$.

Cardinality (Size) of Sets

- **Def^n**: For a set S, if there are exactly n distinct elements in S for some positive integer n, then S is a **finite set** of **cardinality** n, denoted $|S| = n$. A set is **infinite** if it is not finite.
  - **Ex**: $|\{1, 3, 5\}| = 3$
  - **Ex**: | English alphabet | $= 26$
  - **Ex**: $|\emptyset| = 0$
  - **Ex**: $|\{\emptyset\}| = 1$

- Infinite sets have interesting structures on cardinality
  - Size of the set of integers?
  - What about odd numbers?
  - Real numbers?
  - Need “functions” to make this more precise
  - Infinity is weird (and may or may not be real at all!)

Power Set

- **Def^{n}**: The power set of a set S is the set of all subsets of S, denoted $P(S)$
  - **Ex**: $P(\{1,2\}) = ?$
  - **Ex**: $P(\emptyset) = ?$
  - **Ex**: $P(P(\emptyset)) = ?$
  - For a finite set S, $|P(S)| = 2^{|S|}$

Cartesian Products

- **Def^{n}**: The ordered n-tuple $(a_1, \dots, a_n)$ is the ordered collection with a_i being the i-th element.
- **Def^{n}**: The Cartesian product of the sets $A_1, \dots, A_n$, is the set

$$A_1 \times \cdots \times A_n = \{(a_1, \dots, a_n) \mid a_i \in A_i \;\; for \;\; 1 \leq i \leq n\}.$$

- **Ex**: $A = \{1, 2\}, B = \{2, 3\}$. What is $A \times B$?

- Note that $|A_1 \times \cdots \times A_n| = |A_1| \times \cdots \times |A_n|$
- Can be infinite, e.g., the x-y coordinate system

Potential Issues with “Naïve” Set Theory

- Consider $A = \{x \mid x \notin x\}$.
  - That is, set A contains elements that are sets which do not contain themselves.
  - Question: $A \in A$?

Set Operations

- Let U be the "universe"
  - Union: $A \cup B = \{x \mid x \in A \vee x \in B\}$
  - Intersection: $A \cap B = \{x \mid x \in A \wedge x \in B\}$
  - A and B are disjoint if $A \cap B = \emptyset$
  - Difference: $A \backslash \mathrm{B} = A - B = \{x \mid x \in A \wedge x \notin B\}$
  - Complement: $\bar{A} = U - A = \{x \in U \mid x \notin A\}$
  - Symmetric difference: $A \oplus B = (A \cup B) - (A \cap B)$

Set Operations, Cont.

- **Ex**: $U = \{1, \ldots, 10\}$, $A = \{2, 3,6,8,9\}$, $B = \{3,4,8, 10\}$

Set Identities

- Set identities are somewhat like logical operations
- **Ex:** $\overline{A \cap B} = \bar{A} \cup \bar{B}$

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

Set Identities, Cont.

- **Ex:** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Set Identities: Proof using Identities

- **Ex**: $\overline{A \cup (B \cap C)} = \bar{A} \cap (\bar{B} \cup \bar{C})$