Formal Logic

A Pragmatic Introduction
(Based on [Gallier 1986] and [Huth and Ryan 2004])

Yih-Kuen Tsay

Department of Information Management
National Taiwan University

What It Is

IM NTU

- Logic concerns two concepts:
  - truth (in a specific or general context)
  - provability (of truth from assumed truth)
- *Formal (symbolic) logic* approaches logic by rules for manipulating symbols:
  - syntax rules: for writing statements or formulae. (There are also semantic rules determining whether a statement is true or false in a context or mathematical structure.)
  - inference rules: for obtaining true statements from other true statements.
- Two main branches of formal logic:
  - *propositional logic*
  - *first-order logic* (predicate logic/calculus)

Why We Need It (in Software Development)

IM NTU

- Correctness of software hinges on a precise statement of its requirements.
- Logical formulae give the most precise kind of statements about software requirements.
- The fact that "a software program satisfies a requirement" is very much the same as "a mathematical structure satisfies a logical formula":

$$prog \models req \quad \text{vs.} \quad M \models \varphi$$

- To prove that a software program is correct, one may utilize the kind of inferences seen in formal logic.

Propositions

- A *proposition* is a statement that is either *true* or *false* such as the following:
  - Leslie is a teacher.
  - Leslie is rich.
  - Leslie is a pop singer.
- Simplest (atomic) propositions may be combined to form compound propositions:
  - Leslie is *not* a teacher.
  - *Either* Leslie is not a teacher *or* Leslie is not rich.
  - *If* Leslie is a pop singer, *then* Leslie is rich.

Inferences

- We are given the following assumptions:
  - Leslie is a teacher.
  - Either Leslie is not a teacher or Leslie is not rich.
  - If Leslie is a pop singer, then Leslie is rich.
- We wish to conclude the following:
  - Leslie is not a pop singer.
- The above process is an example of *inference* (deduction). Is it correct?

Symbolic Propositions

- Propositions are represented by *symbols*, when only their truth values are of concern.
  - *P*: Leslie is a teacher.
  - *Q*: Leslie is rich.
  - *R*: Leslie is a pop singer.
- Compound propositions can then be more succinctly written.
  - *not P*: Leslie is not a teacher.
  - *not P or not Q*: Either Leslie is not a teacher or Leslie is not rich.
  - *R implies Q*: If Leslie is a pop singer, then Leslie is rich.

Symbolic Inferences

- We are given the following assumptions:
  - P (Leslie is a teacher.)
  - *not* P *or not* Q (Either Leslie is not a teacher or Leslie is not rich.)
  - R *implies* Q (If Leslie is a pop singer, then Leslie is rich.)
- We wish to conclude the following:
  - *not* R (Leslie is not a pop singer.)
- Correctness of the inference may be checked by asking:
  - Is (P *and* (*not* P *or not* Q) *and* (R *implies* Q)) *implies* (*not* R) a tautology (valid formula)?
  - Or, is $P \wedge (\neg P \vee \neg Q) \wedge (R \rightarrow Q) \rightarrow \neg R$ valid?

Models

- *Models* provide the context in which a logic formula is judged to be true or false.
- Models are formally represented as mathematical structures.
- A formula can be true in one model, but false in another.
- A model *satisfies* a formula if the formula is true in the model (notation: $M \models \varphi$).
- A formula is *satisfiable* if there is a model that satisfies the formula.
- A formula is *valid* if it is true in every model (notation: $\models \varphi$).

Semantic Entailment

- Let Γ be a set of formulae.
- A model satisfies Γ if the model satisfies every formula in Γ.
- We say that Γ *semantically entails* C if every model that satisfies Γ also satisfies C, written as $\Gamma \models C$.
  - $A, A \rightarrow B \models B$
  - $A \rightarrow B, \neg B \models \neg A$
- A main ingredient of a logic is a systematic way to draw conclusions of the above form, namely $\Gamma \models C$.

Sequents

- We write "$A_1, A_2, \cdots, A_m \vdash C$" to mean that the truth of formula C follows from the truth of formulae $A_1, A_2, \cdots, A_m$.
- "$A_1, A_2, \cdots, A_m \vdash C$" is called a *sequent*.
- In the sequent, $A_1, A_2, \cdots, A_m$ collectively are called the *antecedent* (also *context*) and C the *consequent*.

Note: Many authors prefer to write a sequent as $\Gamma \longrightarrow C$ or $\Gamma \Longrightarrow C$, while reserving the symbol $\vdash$ for provability (deducibility) in the proof (deduction) system under consideration.

Inference Rules

IM NTU

- Inference rules allow one to obtain true statements from other true statements.
- Below is an inference rule for conjunction.

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \, (\wedge I)$$

- In an inference rule, the upper sequents (above the horizontal line) are called the *premises* and the lower sequent is called the *conclusion*.

Proofs

- A deduction tree is a tree where each node is labeled with a sequent such that, for every internal (non-leaf) node,
  - the label of the node corresponds to the conclusion and
  - the labels of its children correspond to the premises

  of an instance of an inference rule.
- A proof tree is a deduction tree, each of whose leaves is labeled with an axiom.
- The root of a deduction or proof tree is called the conclusion.
- A sequent is provable if there exists a proof tree of which it is the conclusion.

Natural Deduction in the Sequent Form

$$\frac{}{\Gamma, A \vdash A}\ (Ax)$$

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\wedge I)$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ (\wedge E_1)$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ (\wedge E_2)$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\vee I_1)$$

$$\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\vee I_2)$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\ (\vee E)$$

Natural Deduction (cont.)

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ (\to I) \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ (\to E)$$

$$\frac{\Gamma, A \vdash B \wedge \neg B}{\Gamma \vdash \neg A}\ (\neg I) \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash \neg A}{\Gamma \vdash B}\ (\neg E)$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \neg\neg A}\ (\neg\neg I) \qquad \frac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}\ (\neg\neg E)$$

Note: these inference rules collectively are called System *ND*.

Soundness

- A deduction (proof) system is *sound* if it produces only semantically valid results.
- More formally, a system is sound if, whenever $\Gamma \vdash C$ is provable in the system, then $\Gamma \models C$.
- Soundness allows us to draw semantically valid conclusions from purely syntactical inferences.

Predicates

- A *predicate* is a "parameterized" statement that, when supplied with actual arguments, is either *true* or *false* such as the following:
  - Leslie is a teacher.
  - Chris is a teacher.
  - Leslie is a pop singer.
  - Chris is a pop singer.
- Like propositions, simplest (atomic) predicates may be combined to form compound predicates.

Inferences

- We are given the following assumptions:
  - *For any* person, *either* the person is not a teacher *or* the person is not rich.
  - *For any* person, *if* the person is a pop singer, *then* the person is rich.
- We wish to conclude the following:
  - *For any* person, *if* the person is a teacher, *then* the person is not a pop singer.

Symbolic Predicates

- Like propositions, predicates are represented by *symbols*.
  - $p(x)$: x is a teacher.
  - $q(x)$: x is rich.
  - $r(y)$: y is a pop singer.
- Compound predicates can be expressed:
  - For all x, $r(x) \rightarrow q(x)$: *For any* person, *if* the person is a pop singer, *then* the person is rich.
  - For all y, $p(y) \rightarrow \neg r(y)$: *For any* person, *if* the person is a teacher, *then* the person is *not* a pop singer.

Symbolic Inferences

- We are given the following assumptions:
  - For all $x, \neg p(x) \vee \neg q(x)$.
  - For all $x, r(x) \rightarrow q(x)$.
- We wish to conclude the following:
  - For all $x, p(x) \rightarrow \neg r(x)$.
- To check the correctness of the inference above, we ask:
  - is ((for all $x, \neg p(x) \vee \neg q(x)$) $\wedge$ (for all $x, r(x) \rightarrow q(x)$)) $\rightarrow$ (for all $x, p(x) \rightarrow \neg r(x)$) valid?
  - or, is $\forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)) \rightarrow \forall x(p(x) \rightarrow \neg r(x))$ valid?

Theory

IM NTU

- Assume a fixed first-order language.
- A set S of sentences is closed under provability if

$$S = \{A \mid A \text{ is a sentence and } S \vdash A \text{ is provable}\}.$$

- A set of sentences is called a *theory* if it is closed under provability.
- A theory is typically represented by a smaller set of sentences, called its *axioms*.

Note: a sentence is a formula without free variables. For example, $\forall x(x \geq 0)$ is a sentence, but $x \geq 0$ is not.

Group as a First-Order Theory

- The set of non-logical symbols is $\{\cdot, e\}$, where $\cdot$ is a binary function (operation) and e is a constant (the identity).
- Axioms:
  - $\forall a, b, c(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$ (Associativity)
  - $\forall a(a \cdot e = e \cdot a = a)$ (Identity)
  - $\forall a(\exists b(a \cdot b = b \cdot a = e))$ (Inverse)
- $(Z, \{+, 0\})$ is a model of the theory.
- So is $(Q \setminus \{0\}, \{\times, 1\})$.
- Additional axiom for Abelian groups:
  - $\forall a, b(a \cdot b = b \cdot a)$ (Commutativity)

Theorems

- A *theorem* is just a statement (sentence) in a theory (a set of sentences).
- For example, the following are theorems in Group theory:
  - $\forall a \forall b \forall c((a \cdot b = a \cdot c) \to b = c)$.
  - $\forall a \forall b \forall c(((a \cdot b = e) \wedge (b \cdot a = e) \wedge (a \cdot c = e) \wedge (c \cdot a = e)) \to b = c)$, which says that every element has a unique inverse.