

# 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

- 🌐 Logic concerns two concepts:
  - ☀️ **truth** (in a specific or general context/model)
  - ☀️ **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.  
(It is also possible to confirm true statements by considering all possible contexts.)
- 🌐 Two main branches of formal logic:
  - ☀️ **propositional logic**
  - ☀️ **first-order logic** (predicate logic/calculus)

# Why We Need It (in Software Development)

- 🌐 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”:

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

- 🌐 To **prove** (formally verify) that a software program is correct, one may utilize the kind of inferences seen in formal logic.
- 🌐 The verification may be done manually, semi-automatically, or fully automatically.

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

# Boolean Expressions and Propositions

🌐 *Boolean expressions* are essentially propositional formulae, though they may allow more things as atomic formulae.

🌐 Boolean expressions:

☀  $(x \vee y \vee \bar{z}) \wedge (\bar{x} \vee \bar{y}) \wedge x$

☀  $(x + y + \bar{z}) \cdot (\bar{x} + \bar{y}) \cdot x$

☀  $(a \vee b \vee \bar{c}) \wedge (\bar{a} \vee \bar{b}) \wedge a$

☀ etc.

🌐 Propositional formula:  $(P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q) \wedge P$

# Normal Forms

- 🌐 A *literal* is an atomic proposition or its negation.
- 🌐 A propositional formula is in **Conjunctive Normal Form (CNF)** if it is a conjunction of disjunctions of literals.
  - ☀  $(P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q) \wedge P$
  - ☀  $(P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R)$
- 🌐 A propositional formula is in **Disjunctive Normal Form (DNF)** if it is a disjunction of conjunctions of literals.
  - ☀  $(P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q) \vee P$
  - ☀  $(\neg P \wedge \neg Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R)$
- 🌐 A propositional formula is in **Negation Normal Form (NNF)** if negations occur only in literals.
  - ☀ CNF or DNF is also NNF (but not vice versa).
  - ☀  $(P \wedge \neg Q) \wedge (P \vee (Q \wedge \neg R))$  in NNF, but not CNF or DNF.
- 🌐 Every propositional formula has an equivalent formula in each of these normal forms.

# Models, Satisfiability, and Validity

- 🌍 *Models* provide the (semantic) 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:  $M \models \varphi$ ).
  - ☀️  $v(P) = F, v(Q) = T \models (P \vee Q) \wedge (\neg P \vee \neg Q)$
- 🌍 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:  $\models \varphi$ ).
  - ☀️  $\models A \vee \neg A$
  - ☀️  $\models (A \wedge B) \rightarrow (A \vee B)$

# Semantic Entailment

- Let  $\Gamma$  be a set of formulae.
- A model satisfies  $\Gamma$  if the model satisfies every formula in  $\Gamma$ .
- We say that  $\Gamma$  *semantically entails*  $C$  if every model that satisfies  $\Gamma$  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 “ $A_1, A_2, \dots, A_m \vdash C$ ” to mean that the truth of formula  $C$  follows from the truth of formulae  $A_1, A_2, \dots, A_m$ .
- 🌐 “ $A_1, A_2, \dots, A_m \vdash C$ ” is called a *sequent*.
- 🌐 In the sequent,  $A_1, A_2, \dots, A_m$  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

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

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

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

- 🌐 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

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

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

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

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

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

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

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

# Natural Deduction (cont.)

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

$$\frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} (\rightarrow E)$$

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

$$\frac{\Gamma \vdash A \quad \Gamma \vdash \neg A}{\Gamma \vdash B} (\neg E)$$

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

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

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

# A Proof in Propositional ND

Below is a partial proof of the validity of  
 $P \wedge (\neg P \vee \neg Q) \wedge (R \rightarrow Q) \rightarrow \neg R$  in ND,  
 where  $\gamma$  denotes  $P \wedge (\neg P \vee \neg Q) \wedge (R \rightarrow Q)$ .

$$\begin{array}{c}
 \frac{\frac{\frac{\vdots}{\gamma, R \vdash R \rightarrow Q}}{\gamma, R \vdash Q} \quad \frac{\gamma, R \vdash R}{\gamma, R \vdash R} (Ax)}{\gamma, R \vdash Q} (\rightarrow E) \quad \frac{\frac{\frac{\vdots}{\gamma, R, Q \vdash P \wedge \neg P}}{\gamma, R \vdash \neg Q} (\neg I)}{\gamma, R \vdash \neg Q} (\wedge I)}{\gamma, R \vdash Q \wedge \neg Q} (\wedge I)}{\frac{P \wedge (\neg P \vee \neg Q) \wedge (R \rightarrow Q) \vdash \neg R}{\vdash P \wedge (\neg P \vee \neg Q) \wedge (R \rightarrow Q) \rightarrow \neg R} (\rightarrow I)} (\neg I)}
 \end{array}$$

- 🌐 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.

 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  $((\text{for all } x, \neg p(x) \vee \neg q(x)) \wedge (\text{for all } x, r(x) \rightarrow q(x))) \rightarrow (\text{for all } x, p(x) \rightarrow \neg r(x))$  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?

# Free and Bound Variables

- In a formula  $\forall xA$  (or  $\exists xA$ ), the variable  $x$  is *bound* by the quantifier  $\forall$  (or  $\exists$ ).
- A *free* variable is one that is not bound.
- The same variable may have both a free and a bound occurrence.
- For example, consider  $(\forall x(R(x, \underline{y}) \rightarrow P(x)) \wedge \forall y(\neg R(\underline{x}, y) \wedge \forall xP(x)))$ .  
The underlined occurrences of  $x$  and  $y$  are free, while others are bound.
- A formula is *closed*, also called a *sentence*, if it does not contain a free variable.

# Substitutions

- Let  $t$  be a term (such as  $x$ ,  $g(x, y)$ , etc.) and  $A$  a formula.
- The result of substituting  $t$  for a free variable  $x$  in  $A$  is denoted by  $A[t/x]$ .
- Consider  $A = \forall x(P(x) \rightarrow Q(x, f(y)))$ .
  - When  $t = g(y)$ ,  $A[t/y] = \forall x(P(x) \rightarrow Q(x, f(g(y))))$ .
  - For any  $t$ ,  $A[t/x] = \forall x(P(x) \rightarrow Q(x, f(y))) = A$ , since there is no free occurrence of  $x$  in  $A$ .
- A substitution is *admissible* if no free variable of  $t$  would become bound (be captured by a quantifier) after the substitution.
- For example, when  $t = g(x, y)$ ,  $A[t/y]$  is not admissible, as the free variable  $x$  of  $t$  would become bound.

# Quantifier Rules of Natural Deduction

$$\frac{\Gamma \vdash A[y/x]}{\Gamma \vdash \forall x A} (\forall I)$$

$$\frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[t/x]} (\forall E)$$

$$\frac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x A} (\exists I)$$

$$\frac{\Gamma \vdash \exists x A \quad \Gamma, A[y/x] \vdash B}{\Gamma \vdash B} (\exists E)$$

In the rules above, we assume that all substitutions are admissible and  $y$  does not occur free in  $\Gamma$  or  $A$ .

# A Proof in First-Order ND

Below is a partial proof of the validity of  $\forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)) \rightarrow \forall x(p(x) \rightarrow \neg r(x))$  in ND, where  $\gamma$  denotes  $\forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x))$ .

$$\begin{array}{c}
 \vdots \\
 \hline
 \gamma, p(y), r(y) \vdash r(y) \rightarrow q(y) \quad \gamma, p(y), r(y) \vdash r(y) \quad (Ax) \\
 \hline
 \gamma, p(y), r(y) \vdash q(y) \quad (\rightarrow E) \\
 \vdots \\
 \hline
 \forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)), p(y), r(y) \vdash q(y) \wedge \neg q(y) \quad (\wedge I) \\
 \hline
 \forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)), p(y) \vdash \neg r(y) \quad (\neg I) \\
 \hline
 \forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)), p(y) \vdash \neg r(y) \quad (\rightarrow I) \\
 \hline
 \forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)) \vdash p(y) \rightarrow \neg r(y) \quad (\forall I) \\
 \hline
 \forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)) \vdash \forall x(p(x) \rightarrow \neg r(x)) \quad (\rightarrow I) \\
 \hline
 \vdash \forall x(\neg p(x) \vee \neg q(x)) \wedge \forall x(r(x) \rightarrow q(x)) \rightarrow \forall x(p(x) \rightarrow \neg r(x))
 \end{array}$$

# Equality Rules of Natural Deduction

Let  $t, t_1, t_2$  be arbitrary terms; again, assume all substitutions are admissible.

$$\frac{}{\Gamma \vdash t = t} (= I) \qquad \frac{\Gamma \vdash t_1 = t_2 \quad \Gamma \vdash A[t_1/x]}{\Gamma \vdash A[t_2/x]} (= E)$$

Note: The  $=$  sign is part of the object language, not a meta symbol.

# Theory

- 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)
-   $(\mathbb{Z}, \{+, 0\})$  is a model of the theory.
-  So is  $(\mathbb{Q} \setminus \{0\}, \{\times, 1\})$ .
-  Additional axiom for Abelian groups:
  -   $\forall a, b(a \cdot b = b \cdot a)$  (Commutativity)

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