SC/MATH 1090

4- Theorem Calculation

Ref: G. Tourlakis, *Mathematical Logic*, John Wiley & Sons, 2008.

York University

Department of Computer Science and Engineering

Overview

- Logical axioms
- Rules of inference
- Theorem Calculations, or Proofs
- Hilbert-style Proofs

Logical axioms of Boolean Logic

	Properties of $\equiv$	
Associativity of $\equiv$	$((A \equiv B) \equiv C) \equiv (A \equiv (B \equiv C))$	(1)
Symmetry of $\equiv$	$(A \equiv B) \equiv (B \equiv A)$	(2)
	Properties of $\bot, \top$	
$\top$ vs. $\bot$	$\top \equiv \bot \equiv \bot$	(3)
	Properties of $\neg$	
Introduction of $\neg$	$\neg A \equiv A \equiv \bot$	(4)
	Properties of $\vee$	
Associativity of $\vee$	$(A \vee B) \vee C \equiv A \vee (B \vee C)$	(5)
Symmetry of $\vee$	$A \vee B \equiv B \vee A$	(6)
Idempotency of $\vee$	$A \vee A \equiv A$	(7)
Distributivity of $\vee$ over $\equiv$	$A \vee (B \equiv C) \equiv A \vee B \equiv A \vee C$	(8)
Excluded Middle	$A \vee \neg A$	(9)
	Properties of $\wedge$	
Golden Rule	$A \wedge B \equiv A \equiv B \equiv A \vee B$	(10)
	Properties of $\rightarrow$	
Implication	$A \rightarrow B \equiv A \vee B \equiv B$	(11)

Axioms

- We will use the capital Greek letter "lambda" , Λ, to denote the set of all **logical axioms**.
- Note that since the logical axioms (shown in previous slide) are schemata, Λ is infinite.
- All **assumptions or hypotheses** for a specific problem, are called **special axioms** or **nonlogical axioms** and are denoted by "gamma", Γ.
- Note that Γ is not fixed.

Primary Rules of Inference

$$\frac{A, A \equiv B}{B} \qquad (Eqn)$$

$$\frac{A \equiv B}{C[\mathbf{p} := A] \equiv C[\mathbf{p} := B]} \qquad (Leib)$$

- The numerator shows the **premises**, **hypotheses**, or **assumptions**.
- The denominator shows the **conclusion** or **result** of the rule.
- The first rule is the rule of Equanimity or Eqn.
- The second rule is the Leibniz rule or Leib.

Theorem Calculations, or Γ-Proofs

- Let Γ be a given set of formulae (our assumptions)
- A theorem-calculation (or proof) from Γ is any finite (ordered) sequence of formulae that can be written following these rules:
  1. We may write a formula from Λ or Γ at any step
  2. We may write the denominator of an *instance of an inference rule*, provided all formulae in the numerator (of the same instance) have been written in a previous step.

Theorem

- **Definition. (Theorems)** Any formula A that appears in a Γ-proof is called a Γ-theorem. This is denoted by $\Gamma \vdash A$.
  - The above proof is said to prove A from Γ.
  - If $\Gamma = \emptyset$ (empty set), we write $\vdash$ A, and call A just a theorem or an absolute theorem, or logical theorem.

Hilbert-Style Proof - framework

- To Prove $\Gamma \vdash A$:

  (1) ...... <annotation>

  (2) ...... <annotation>

  (n) A <annotation>

  Steps in a theorem calculation

- Annotations explain the step written in a proof.
- In a Hilbert style proof, conclusion appears at the last step (although by definition, it is not wrong to have more (unnecessary!) steps).

Some simple theorems

a) $\vdash A \vee \neg A$

b) $A \vdash A$

c) $A, A \equiv B \vdash B$

d) $A \equiv B \vdash C[\mathbf{p}:=A] \equiv C[\mathbf{p}:=B]$

e) $A \equiv B, B \equiv C \vdash A \equiv C$ **Transitivity**

f) $\vdash A \equiv A$

Strengthening metatheorems!

- **Metatheorem. (Hypothesis Strengthening)** If $\Gamma \vdash A$ and $\Gamma \subseteq \Delta$, then also $\Delta \vdash A$.
  - If $\vdash A$, then also $\Gamma \vdash A$ for any set of formulae Γ.

- **Metatheorem. (Transitivity of ⊢)** Assume we have
  $\Gamma \vdash B_1, \Gamma \vdash B_2, \ldots, \Gamma \vdash B_n$
  and $B_1, B_2, \ldots, B_n \vdash A$
  Then $\Gamma \vdash A$.

- **Corollary.** If $\Gamma \cup \{A\} \vdash B$ and also $\Gamma \vdash A$, then $\Gamma \vdash B$.

- **Corollary.** If $\Gamma \cup \{A\} \vdash B$ and also $\vdash A$, then $\Gamma \vdash B$.

More tools for our toolbox

a) $B, A \equiv B \vdash A$ **The other Eqn!**

b) $\vdash \bot \equiv \bot$

c) $\vdash \top$

d) $C[p:=A], A \equiv B \vdash C[p:=B]$ **Eqn + Leib merged**

e) $\vdash (A \equiv (B \equiv C)) \equiv ((A \equiv B) \equiv C)$

f) $\vdash A \equiv A \equiv B \equiv B$

- $\vdash \bot \equiv \bot \equiv B \equiv B$
- $\vdash A \equiv A \equiv \bot \equiv \bot$

Redundant True

- **Redundant True Theorem:**

  $\vdash \top \equiv A \equiv A$ and $\vdash A \equiv A \equiv \top$

- **(Redundant True) Metatheorem**.

  For any Γ and A, $\Gamma \vdash A$ iff $\Gamma \vdash A \equiv \top$.

  – Special case: $A \vdash A \equiv \top$

- **Metatheorem**. For any Γ, A, and B, if $\Gamma \vdash A$ and $\Gamma \vdash B$, then $\Gamma \vdash A \equiv B$.