SC/MATH 1090

4- Theorem Calculation


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 $\equiv$  \[(A \equiv B) \equiv C \equiv (A \equiv (B \equiv C))\]  \hspace{1cm} (1)

Symmetry of $\equiv$  \[(A \equiv B) \equiv (B \equiv A)\]  \hspace{1cm} (2)

Properties of $\bot, \top$

$\top$ vs. $\bot$  \[\top \equiv \bot \equiv \bot\]  \hspace{1cm} (3)

Properties of $\neg$

Introduction of $\neg$  \[\neg A \equiv A \equiv \bot\]  \hspace{1cm} (4)

Properties of $\lor$

Associativity of $\lor$  \[(A \lor B) \lor C \equiv A \lor (B \lor C)\]  \hspace{1cm} (5)

Symmetry of $\lor$  \[A \lor B \equiv B \lor A\]  \hspace{1cm} (6)

Idempotency of $\lor$  \[A \lor A \equiv A\]  \hspace{1cm} (7)

Distributivity of $\lor$ over $\equiv$  \[A \lor (B \equiv C) \equiv A \lor B \equiv A \lor C\]  \hspace{1cm} (8)

Excluded Middle  \[A \lor \neg A\]  \hspace{1cm} (9)

Properties of $\land$

Golden Rule  \[A \land B \equiv A \equiv B \equiv A \lor B\]  \hspace{1cm} (10)

Properties of $\rightarrow$

Implication  \[A \rightarrow B \equiv A \lor B \equiv B\]  \hspace{1cm} (11)
Axioms

• We will use the capital Greek letter "lambda", \( \Lambda \), to denote the set of all logical axioms.

• Note that since the logical axioms (shown in previous slide) are schemata, \( \Lambda \) is infinite.

• All assumptions or hypotheses for a specific problem, are called special axioms or nonlogical axioms and are denoted by "gamma", \( \Gamma \).

• Note that \( \Gamma \) is not fixed.
Primary Rules of Inference

\[
\frac{A, A \equiv B}{B} \quad (Eqn)
\]

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

- 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 $\Gamma$-Proofs

- Let $\Gamma$ be a given set of formulae (our assumptions)

- A theorem-calculation (or proof) from $\Gamma$ is any finite (ordered) sequence of formulae that can be written following these rules:
  1. We may write a formula from $\Lambda$ or $\Gamma$ 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 $\Gamma$-proof is called a $\Gamma$-**theorem**. This is denoted by $\Gamma \vdash A$.
  
  - The above proof is said to **prove** $A$ from $\Gamma$.
  
  - 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) \( \vdash A \lor \neg A \)

b) \( A \vdash A \)

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

d) \( A \equiv B \vdash C[p:=A] \equiv C[p:=B] \)

e) \( A \equiv B, B \equiv C \vdash A \equiv C \) \hspace{1cm} \text{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 $\Gamma$.

• **Metatheorem. (Transitivity of $\vdash$)** Assume we have
  
  $\Gamma \vdash B_1$, $\Gamma \vdash B_2$, ..., $\Gamma \vdash B_n$
  
  and $B_1, B_2, ..., B_n \vdash A$
  
  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) \( B, A \equiv B \vdash A \)  

b) \( \vdash \bot \equiv \bot \)

c) \( \vdash T \)

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:**

  \[ \vdash T \equiv A \equiv A \text{ and } \vdash A \equiv A \equiv T \]

- **(Redundant True) Metatheorem.**
  For any \( \Gamma \) and \( A \), \( \Gamma \vdash A \iff \Gamma \vdash A \equiv T \).
  
  – Special case: \( A \vdash A \equiv T \)

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