

# CMSC 31100 Week 7: Logic in CS/CS in Logic

Lecturer: David MacQueen

November 11, 2006

## 1. Models of computation---Computability (Church thesis)

- Computability Theory
- Complexity theory/ theory of algorithms
- Theory of Programming (Languages)
  
- Programming Logics
- Mechanizing Logics
- Type Theory (Constructive Logic)
- Modal/Temporal Logics

## 2. Hoare Logic

$e$  — integer expression

$1, 2, \dots, |x| e_1 + e_2 | \dots$

$b$  — boolean expression

$\text{true} | \text{false} \quad e_1 = e_2 \quad e_1 < e_2 \quad \dots$

$|\neg b| b_1 \vee b_2 \quad b_1 \wedge b_2 \quad \dots$

$c$ -commands

$x_i = e \quad c_1; c_2 \quad \text{if } b \text{ then } c_1 \text{ else } c_2$

$\text{while } b \text{ do } c$

$\{p\} c \{q\}$  --- Hoare triple, this is partial correctness. When  $c$  does not terminate, there is no guarantee.

$p \rightarrow q$

Rules:

$\{q[e/x]\} x:=e \{q\}$

$\{(x-y)>3\} x:=x-y \{x>3\}$

Sequence

$\{p\} c_1; c_2 \{q\}$

$\{p\} c_1 \{r\} \{r\} c_2 \{q\}$

Conditional

$\{p\} \text{if } b \text{ then } c_1 \text{ else } c_2 \{q\}$

$\{b \wedge p\} c_1 \{q\} \quad \{\neg b \wedge p\} c_2 \{q\}$

While

$\{p \wedge b\} c \{p\}$

$\{p\} \text{ while } b \text{ do } c \{ \neg b \wedge p \}$

### 3. Mechanizing Logic

Mechanized Proof

		Model	Logic
Automath	deBruijn	checking	type theory
Boyer-Moore Thm Prover	Robinson	automatic	predictive calculus
Resolution Theorem Proving		automatic	"lisp"
LCF(Logic for Computable functions)		interactive	LCF
$\lambda$ -calculus			

ML --- tactics, tacticals

HOL	(Gordan)	Interactive HOL
NuPRL	(Constable)	Type theory
COQ	(Huet, Coquand)	Type theory
Isabelle	(Paulson)	Type theory
ELF	(Plotkin, Harper, Pfenning)	Type theory

Applications: PCC, meta theory, checking "real" mathematics

$$\begin{array}{l} A \rightarrow B \\ f : A \rightarrow B \\ x \in A \quad | - \quad b \in B \end{array}$$


---


$$| - \lambda x \in A. b : A \rightarrow B$$

$$a \in A \quad b \in B$$


---


$$\langle a, b \rangle \in A \wedge B$$

$$A \rightarrow B \leftrightarrow A \rightarrow B$$

$$A \wedge B \leftrightarrow A \times B$$

$$A \vee B \leftrightarrow A + B$$

$$x \in A$$


---


$$\text{inl}(x) \in A \vee B$$

$$x \in B$$


---


$$\text{inr}(x) \in A \vee B$$

$$\neg A \equiv A \rightarrow \text{False}$$

Example

$A \rightarrow (B \rightarrow A)$

$a \in A \mid - a \in A$

---

$b \in B, a \in A \mid a \in A$

---

$a \in A \mid - \lambda b \in B. a \in B \rightarrow A$

---

$\mid - \lambda b \in A \lambda b \in B. a \in A \rightarrow B \rightarrow A$

$K = \lambda x. \lambda y. x$