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,…., | x | $e_1 + e_2$ |….

b — boolean expression
true | false $e_1 = e_2$ | $e_1 < e_2$ | …

$| \neg b |$ $b_1 \vee b_2$ | $b_1 \wedge b_2$ | …

c-commands
$x_i = e$ | $c_1; c_2$ | if b then c_1 else c_2
while b do c

{p} c {q} --- Hoare triple, this is partial correctness. When c does not terminate, there is no guarantee.
p→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 } if b then c_1 else c_2 { q }
{ $b \wedge p$ } c_1 { q }   { $\neg b \wedge p$ } c_2 { q }

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

{p} while b 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

λ-calculus

ML --- tactics, tacticals

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

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

$$\mathrm{A} \rightarrow \mathrm{B}$$
$$\mathrm{f} : \mathrm{A} \rightarrow \mathrm{B}$$
$$x \in A \quad |\!- \quad \mathrm{b} \in \mathrm{B}$$

$$|\!- \ \lambda x \in A. \ \ \mathrm{b} : \mathrm{A} \rightarrow \mathrm{B}$$

$$\mathrm{a} \in \mathrm{A} \quad \mathrm{b} \in \mathrm{B}$$

$$\langle \mathrm{a}, \mathrm{b} \rangle \in \mathrm{A} \wedge \mathrm{B}$$

$$\mathrm{A} \rightarrow \mathrm{B} \leftrightarrow \mathrm{A} \rightarrow \mathrm{B}$$
$$\mathrm{A} \wedge \mathrm{B} \leftrightarrow \mathrm{A} \times \mathrm{B}$$
$$\mathrm{A} \vee \mathrm{B} \leftrightarrow \mathrm{A} + \mathrm{B}$$

$x \in A$	$x \in B$
-----------------	-------------------
$inl(x) \in A \vee B$	$inr(x) \in A \vee B$

$$\neg A \equiv A \rightarrow False$$

Example

$A \to (B \to A)$

$a \in A \ \ |- \ \ a \in A$

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

$a \in A \ \ |- \ \ \lambda b \in B. \ \ a \in B \to A$

$|- \ \ \lambda b \in A. \ \ \lambda b \in B. \ a \in A \to B \to A$

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