UPMC Paris Universitas – Master Informatique – STL

Cours Composant
6. Logique de Hoare 1

©2005-2013 Frédéric Peschanski

UPMC Paris Universitas

4 mars 2013

Plan du cours

Logique de Hoare I

- Le langage J-While
- Triplets de Hoare
- Axiome d'affectation
- Règle de séquencement
- Opérateurs logiques
- Alternatives

Le langage J-While

Langage J-While : version très simplifiée de Java

- « Programme » = Corps d'une méthode
- pas d'invocation
- types booléens, entiers et tableaux
- expressions arithmétiques et logiques de base
- instructions : affectations, séquencement, alternatives et boucles while

Triplets de Hoare

Triplet de Hoare

{P} prog {Q}

où

- P est la précondition
- prog est un extrait de programme J-While
- Q est la postcondition

Interprétation :

> « *En supposant P vraie avant exécution, et si on exécute prog, alors Q est vraie après exécution* »

Axiome d'affectation

Axiome d'affecation

$$\frac{}{\{Q[\mathrm{expr}/V]\}\ \mathtt{V} = \mathtt{expr}\ \{Q\}}\ (\mathit{aff})$$

Remarque :
$Q[\mathrm{expr}/V] \stackrel{def}{=} Q$ en substituant toute occurence libre de V dans Q par expr (ou expr « écrase » V dans Q)

Axiome d'affectation : exemples

Axiome d'affecation

$$\frac{}{\{Q[\mathrm{expr}/V]\}\ \mathtt{V} = \mathtt{expr}\ \{Q\}}\ (aff)$$

Exercice 1 : On cherche la précondition la plus faible P telle que

$$\{P\}\mathtt{x} = \mathtt{y} + 1\{x = 3\}$$

Exercice 2 : Trouver P et Q « intéressantes » telles que

$$\{P\}\mathtt{x} = -\mathtt{y}\{Q\}$$

Exercice 3 : Trouver `prog` tel que

$$\{y = a\}\mathtt{prog}\{y = a \land x = 2 * a\}$$

Règle de séquencement

Règle de séquencement

$$\frac{\{P\}\ \mathtt{C}_1\ \{Q_1\} \quad \{Q_1\}\ \mathtt{C}_2\ \{Q_2\} \quad \ldots \quad \{Q_{n-1}\}\ \mathtt{C}_n\ \{Q\}}{\{P\}\ \mathtt{C}_1; \ldots; \mathtt{C}_n\ \{Q\}}\ (seq)$$

Exercice : Prouver que

$$\{\mathtt{true}\}\mathtt{z} = \mathtt{x}; \mathtt{z} = \mathtt{z} + \mathtt{y}; \mathtt{u} = \mathtt{z}\{u = x + y\}$$

Opérateurs logiques : rappels

Tables de vérité :

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \implies B$	$\neg A \vee B$	$A \iff B$
false	*false*	*true*	*false*	*false*	*true*	*true*	*true*
false	*true*	*true*	*false*	*true*	*true*	*true*	*false*
true	*false*	*false*	*false*	*true*	*false*	*false*	*false*
true	*true*	*false*	*true*	*true*	*true*	*true*	*true*

Question transposition de la logique classique en logique de Hoare ?

Règles du modus-ponens

$$\frac{P \implies P' \quad \{P'\}\ \mathtt{c}\ \{Q'\} \quad Q' \implies Q}{\{P\}\ \mathtt{c}\ \{Q\}}\ (mp)$$

$$\frac{P \implies P' \quad \{P'\}\ \mathtt{c}\ \{Q\}}{\{P\}\ \mathtt{c}\ \{Q\}}\ (mp\text{-}pre)$$

$$\frac{\{P\}\ \mathtt{c}\ \{Q'\} \quad Q' \implies Q}{\{P\}\ \mathtt{c}\ \{Q\}}\ (mp\text{-}post)$$

Exercice prouver de deux façons : $\{x = 3\}\mathtt{y} = \mathtt{x} + 1\{y > 0\}$

Conjonctions et disjonction

Règle de conjonction

$$\frac{\{P_1\}\ \mathtt{C}\ \{Q_1\} \quad \{P_2\}\ \mathtt{C}\ \{Q_2\}}{\{P_1 \wedge P_2\}\ \mathtt{C}\ \{Q_1 \wedge Q_2\}}\ (conj)$$

Règles de disjonction

$$\frac{\{P_1\}\ \mathtt{C}\ \{Q_1\}}{\{P_1 \vee P_2\}\ \mathtt{C}\ \{Q_1 \vee Q_2\}}\ (disj_1) \qquad \frac{\{P_2\}\ \mathtt{C}\ \{Q_2\}}{\{P_1 \vee P_2\}\ \mathtt{C}\ \{Q_1 \vee Q_2\}}\ (disj_2)$$

Règle des alternatives

Règle des alternatives

$$\frac{\{B \wedge P\}\ \mathtt{C}_1\ \{Q\} \quad \{\neg B \wedge P\}\ \mathtt{C}_2\ \{Q\}}{\{P\}\ \mathtt{if(B)}\ \mathtt{C}_1\ \mathtt{else}\ \mathtt{C}_2\ \{Q\}}\ (alt)$$

Technique de preuve

1. Chercher P_1 telle que $\{P_1\}\mathtt{C}_1\{Q\}$
2. Chercher P_2 telle que $\{P_2\}\mathtt{C}_2\{Q\}$
3. La précondition recherchée est $P \stackrel{def}{=} (B \implies P_1) \wedge (\neg B \implies P_2)$

Règle des alternatives

$$\frac{\{B \wedge P\}\ \mathtt{C}_1\ \{Q\} \quad \{\neg B \wedge P\}\ \mathtt{C}_2\ \{Q\}}{\{P\}\ \mathtt{if(B)}\ \mathtt{C}_1\ \mathtt{else}\ \mathtt{C}_2\ \{Q\}}\ (alt)$$

Exercice 1 Trouver P telle que
$\{P\}$ if(x<y) x=y else x=2 $\{x = 2\}$

Exercice 2 Prouver :
$\{true\}$
a=x+1 ; if((a-1)==0) y=1 else y=a
$\{y = x + 1\}$