LIFLC – Logique classique

CM8 – Preuves de programme: logique de Hoare

Licence informatique UCBL – Automne 2018–2019

https://liris.cnrs.fr/ecoquery/dokuwiki/doku.php?id=enseignement:logique:start

Dpt Informatique

Prouver un programme

Objectif : assurer qu'il fait ce que l'on veut

- Bien **spécifier** $\rightarrow$ logique
- Connaître le langage $\rightarrow$ sémantique
- Prouver $\rightarrow$ systèmes de déduction syntaxique

Software Foundations

Livre en ligne sur les langages de programmation

Écrit en Coq + commentaires $\leftarrow$ livre "exécutable"

Sert de base à ce cours

https://softwarefoundations.cis.upenn.edu/

Assertions

Pouvoir dire quelque chose sur un programme

Formule à vérifier (???) sur un programme

Plutôt à un endroit précis

`assert` : Java, Python, C++, etc + bibliothèques de tests

Assertions

Pouvoir dire quelque chose sur un programme

Formule à vérifier (? ? ?) sur un programme

Plutôt à un endroit précis

`assert` : Java, Python, C++, etc + bibliothèques de tests

Assertions

Pouvoir dire quelque chose sur un programme

Formule à vérifier (???) sur un programme

Plutôt à un endroit précis

`assert` : Java, Python, C++, etc + bibliothèques de tests

Assertions

Pouvoir dire quelque chose sur un programme

Formule à vérifier (???) sur un programme

Plutôt à un endroit précis

`assert` : Java, Python, C++, etc + bibliothèques de tests

Lien programme/assertion

Assertions portant sur les variables du programme

- Plus d'autres variables quantifiées

Formules : caractérisation de l'état

- à un moment particulier

Analogie avec le *debugger* :

- debugger : accès aux variables en cours d'exécution
- formule : caractérisation statique de ces valeurs

Exemple

```
Z ::= X;;
Y ::= 1;;
WHILE not (Z = 0) DO
  Y ::= Y * Z;;
  Z ::= Z - 1
END
```

Contraintes sur les valeurs des variables :

- $X \doteq 5 \land Y \doteq 1$
- $\mathit{inf}(0, Z) \land \neg(0 \doteq Z)$

Formules vraies

- à quel point du programme ?
- pour quelle conditions initales ?

Pré/post-conditions

Valeur des formules
$\leftarrow$ valeur des variables
$\leftarrow$ valeur initiale des variables + avancement dans le programme

Programme = transformateur d'état

- Assertions valables avant exécution (pré-conditions)
- induisent après exécution d'autres assertions (post-conditions)

Triplets de Hoare

Syntaxiquement :

$$\{\{\textit{pré-condition}\}\} \quad \texttt{programme} \quad \{\{\textit{post-condition}\}\}$$

Comment raisonner ?
i.e. prouver que :

la transformation du programme
$+$
la pré-condition
$\Rightarrow$
la post-condition

Système de règles pour la preuve de programmes

$$\text{Jugement} = \text{triplet de Hoare}$$

correct si :

- la post condition est vraie
- sur l'état transformé par le programme
- lorsque la précondition est vraie

Definition (Correction d'un triplet de Hoare)

Un triplet de Hoare $\{\{A\}\} \quad P \quad \{\{B\}\}$ est correct si

- pour toute valuation ζ
- si $eval(I, \zeta)(A) = 1$ et si $P : \zeta \rightsquigarrow \zeta'$
- alors

$$eval(I, \zeta')(B) = 1$$

Digression : interprétations et théories

- Fixer I peu commode pour raisonner
- Théorie Th : ensemble de formules
  - servant d'hypothèse de travail
  - *i.e.* on se place uniquement dans des interprétations où elles sont vérifiées
- Th utilisable pour raisonner

Exemple

si

- $\forall x \ \mathit{inf}(x, s(x)) \in Th$
- et $\forall x \ \mathit{plus}(1, x) \doteq s(x) \in Th$

alors

$$Th \models (u \doteq \mathit{plus}(1, v)) \Rightarrow \mathit{inf}(v, u)$$

Correction des triplets de Hoare - v2

On suppose une théorie Th telle que $I \models Th$, avec I utilisée pour définir la sémantique opérationnelle de *Imp*.

Definition (Correction d'un triplet de Hoare)

Un triplet de Hoare $\{\{A\}\} \quad P \quad \{\{B\}\}$ est correct si

- pour toute valuation ζ et toute interprétation $I \models Th$
- si $eval(I, \zeta)(A) = 1$ et si $P : \zeta \rightsquigarrow \zeta'$
- alors

$$eval(I, \zeta')(B) = 1$$

On peut en particulier toujours ajouter des éléments de Th dans A ou dans B sans changer la correction d'un triplet de Hoare

Instructions (rappel)

Ensemble inductif des programmes `prog`

- `CSkip`
- `CAss`(x, e) si $x \in \mathcal{V}$ et $e \in$ `aexp`
- `CSeq`(p_1, p_2) si p_1 et p_2 sont des programmes
- `CIf`(b, p_1, p_2) si $b \in$ `bexp` et si p_1 et p_2 sont des programmes
- `CWhile`(b, p) si $b \in$ `bexp` et si p est un programme.

Grammaire (*c.f.* LIFLF) :

$C \rightarrow$ `SKIP | x ::= A | C ;; C | IF B THEN C ELSE C FI`
`| WHILE B DO c END`
$A \rightarrow \ldots$ (expressions arithmétiques)
$B \rightarrow \ldots$ (expressions booléennes)

Règles de déduction sur les triplets de Hoare - SKIP

$$\frac{}{\{\{A\}\}\quad \texttt{CSkip}\quad \{\{A\}\}}\ (\mathcal{H}_{Skip})$$

Règles de déduction sur les triplets de Hoare - : :=

Règle tentante, mais fausse :

$$\frac{}{\{\{\top\}\} \quad \mathtt{CAss}(X, e) \quad \{\{X \doteq e\}\}}$$

Contre-exemple :

$$\frac{}{\{\{\top\}\} \quad \mathtt{CAss}(X, plus(X, 1)) \quad \{\{X \doteq plus(X, 1)\}\}}$$

Notation : $\top = \bot \Rightarrow \bot$

Règles de déduction sur les triplets de Hoare - : :=

$$\frac{}{\{\{A[X := e]\}\} \quad \texttt{CAss}(X, e) \quad \{\{A\}\}} \; (\mathcal{H}_{::=})$$

Exemple :

$$\frac{}{\{\{\mathit{inf}(0, \mathit{plus}(1, X))\}\} \quad \texttt{CAss}(X, \mathit{plus}(1, X)) \quad \{\{\mathit{inf}(0, X)\}\}} \; (\mathcal{H}_{::=})$$

Assouplir les formules utilisables : $\Rightarrow$

$$\frac{\{\{A\}\} \quad \mathtt{P} \quad \{\{B\}\}}{\{\{A'\}\} \quad \mathtt{P} \quad \{\{B'\}\}}\ (\mathcal{H}_{\Rightarrow})$$

si $Th \models A' \Rightarrow A$
et $Th \models B \Rightarrow B'$

⚠ sens des $\Rightarrow$ ⚠

Règles de déduction sur les triplets de Hoare - ; ;

$$\frac{\{\{A\}\} \quad \mathtt{P}_1 \quad \{\{B\}\} \qquad \{\{B\}\} \quad \mathtt{P}_2 \quad \{\{C\}\}}{\{\{A\}\} \quad \mathtt{CSeq}(\mathtt{P}_1, \mathtt{P}_2) \quad \{\{C\}\}}\ (\mathcal{H}_{;;})$$

Règles de déduction sur les triplets de Hoare - IF

$$\frac{\{\{A \land b \doteq \texttt{BTrue}\}\} \quad \texttt{P}_1 \quad \{\{B\}\} \quad \{\{A \land b \doteq \texttt{BFalse}\}\} \quad \texttt{P}_2 \quad \{\{B\}\}}{\{\{A\}\} \quad \texttt{CIf}(\texttt{b}, \texttt{P}_1, \texttt{P}_2) \quad \{\{B\}\}} \; (\mathcal{H}_{IF})$$

$b \doteq \texttt{BTrue}/\texttt{BFalse}$: utilisé pour prendre en compte le résultat du test dans la preuve

Règles de déduction sur les triplets de Hoare - WHILE

$$\frac{\{\{A \wedge b \doteq \texttt{BTrue}\}\} \quad \texttt{P} \quad \{\{A\}\}}{\{\{A\}\} \quad \texttt{CWhile}(b, \texttt{P}) \quad \{\{A \wedge b \doteq \texttt{BFalse}\}\}} \; (\mathcal{H}_{WHILE})$$

Annotation de programmes

Représenter des triplets de Hoare dans un programme

- ajouter une assertion avant et après chaque instruction
- fusionner les assertions identiques qui se suivent

X : := 3

; ;

Y : := X + 2

Annotation de programmes

Représenter des triplets de Hoare dans un programme

- ajouter une assertion avant et après chaque instruction
- fusionner les assertions identiques qui se suivent

$\{\{inf(3, plus(3, 2))\}\}$
X : := 3
$\{\{inf(X, plus(X, 2))\}\}$
; ;

Y : := X + 2

Annotation de programmes

Représenter des triplets de Hoare dans un programme

- ajouter une assertion avant et après chaque instruction
- fusionner les assertions identiques qui se suivent

$\{\{inf(3, plus(3, 2))\}\}$
X : := 3
$\{\{inf(X, plus(X, 2))\}\}$
; ;
$\{\{inf(X, plus(X, 2))\}\}$
Y : := X + 2
$\{\{inf(X, Y)\}\}$

Annotation de programmes

Représenter des triplets de Hoare dans un programme

- ajouter une assertion avant et après chaque instruction
- fusionner les assertions identiques qui se suivent

$\{\{inf(3, plus(3, 2))\}\}$
$\{\{inf(3, plus(3, 2))\}\}$
$\mathsf{X} : := 3$
$\{\{inf(X, plus(X, 2))\}\}$
$;;$
$\{\{inf(X, plus(X, 2))\}\}$
$\mathsf{Y} : := \mathsf{X} + 2$
$\{\{inf(X, Y)\}\}$
$\{\{inf(X, Y)\}\}$

Annotation de programmes

Représenter des triplets de Hoare dans un programme

- ajouter une assertion avant et après chaque instruction
- fusionner les assertions identiques qui se suivent

$\{\{inf(3, plus(3, 2))\}\}$
$\{\{inf(3, plus(3, 2))\}\}$
$\mathsf{X} :\, := 3$
$\{\{inf(X, plus(X, 2))\}\}$
; ;
$\{\{inf(X, plus(X, 2))\}\}$
$\mathsf{Y} :\, := \mathsf{X} + 2$
$\{\{inf(X, Y)\}\}$
$\{\{inf(X, Y)\}\}$