

Nada Abdallah, Cédric Saule, Delphine Longuet
Prof. Burkhardt Wolff
Parc Orsay Université
4, rue Jacques Monod
Building H / Room 012

VERIFICATION PAR PREUVE I

Date : 30.3.2010

Exercice 1 (Formal Verification by Hoare Logic/*Logique de Hoare*)

Derive the following Hoare triples using inference rules introduced during the course :

Dériver les triplets de Hoare suivant en utilisant les règles d'inférence introduites dans le cours.

1. $\vdash \{x \leq 0\} \ x ::=x-1 \ \{x < 0\}$
2. $\vdash \{x \geq 0\} \ \text{WHILE } x \geq 0 \ \text{DO } x ::=x-1 \ \{x = -1\}$
3. $\vdash \{\text{false}\} \ z ::=15 ; z :== -z \ \{z = 15\}$
4. $\vdash \{i < 0 \wedge tm = 1 \wedge sum = 0\} \ \text{PROG } \{sum < i * i\}$
where $\text{PROG} \equiv \text{WHILE } i=0 \ \text{DO } (i::=i - 1 ; tm::= tm + 2 ; sum::=tm + sum)$.

Hints/Indications : In particular, this means :/ *En particulier, on demande de :*

1. use also the derived rules in the rule-set,,
2. construct the derivation tree wrt. to this Hoare-Calculus from the given Hoare-Triple as root to the leaves,
Construire l'arbre de dérivation du calcul de Hoare en partant du triplet à démontrer à la racine jusqu'aux feuilles
3. annotate the rule applications with the correct rule name,
annoter chaque application de règle avec le nom correspondant.
4. use predicate abbreviations in order to keep the proof small and clearly arranged (these abbreviations should be defined below, of course), and
introduire des notations pour les prédicats afin de garder des arbres concis et lisibles (ces abréviations devront bien entendues être définies à côté) , et
5. interpret the result./ *interpréter les résultats.*

Exercice 2 (Hoare Logic)

Derive the following Hoare triples using inference rules introduced during the course :

1. $\vdash \{x \geq 0\} \ x ::=x+1 \ \{x \geq 0\}$

2. $\vdash \{x \leq 0\} \text{ WHILE } x < 0 \text{ DO } x ::= x+1 \{x = 0\}$
3. $\vdash \{\text{false}\} x ::= x*x \{x = 0\}$

Exercise 3 (Square root derivation)

We prove the loop of the "square-root" : The program is given by :

$$\text{PRELUDE} \equiv tm ::= 1; (sum ::= 1; i ::= 0)$$

$$\begin{aligned} \text{PROG} \equiv & \text{WHILE } sum \leq a \text{ DO} \\ & (i ::= i + 1; \\ & tm ::= tm + 2; \\ & sum ::= tm + sum) \end{aligned}$$

1. formulate the complete specification as pre-and post condition
2. state the Hoare-triple to be proven
3. prove the proof for the PRELUDE
4. prove the proof for PROG