

Spécification et preuve de programmes

Devoir 1 : Vérification déductive, logique de Hoare et logique de micro-C

Alain Giorgetti

Licence d'Informatique de l'Université de Franche-Comté 2020-21

Un barème est donné à titre indicatif.

Afin que ce devoir serve aussi d'entraînement aux examens, il est demandé que toutes les réponses soient rédigées **à la main** par l'étudiant.e, sur des feuilles au format A4 portant chacune le nom et le prénom de l'étudiant.e. Ces feuilles doivent être numérisées au format PDF, par scan ou photographie, et déposées sur Moodle dans le devoir prévu à cet effet.

1 Preuve propositionnelle avec micro-C (2 points)

Donner le contenu d'un fichier micro-C qui permet de démontrer avec l'interface en ligne que les formules $(p \Rightarrow q) \vee r$ et $p \Rightarrow (q \vee r)$ sont équivalentes.

2 Logique des prédicats avec micro-C (6 points)

Sachant que :

- (H_1) tout homme est un primate ;
- (H_2) les dauphins ne sont pas des primates ;
- (H_3) il y a des dauphins intelligents.

on veut aboutir à la conclusion (C) qu'on peut ne pas être un homme et être intelligent.

1. Les prédicats $h(x)$, $p(x)$, $d(x)$ et $i(x)$ formalisent respectivement les propositions “ x est un homme”, “ x est un primate”, “ x est un dauphin” et “ x est intelligent”.

Utiliser ces prédicats pour formaliser les hypothèses (H_1) , (H_2) et (H_3) et la conclusion (C) du problème par des formules closes du premier ordre.

2. Présenter le problème comme une seule formule du premier ordre dont on doit prouver la validité.
3. Formaliser ce problème dans la logique de micro-C.
4. Décrire la réponse de l'interface en ligne de micro-C pour ce problème.

3 Définitions de la valeur absolue d'un entier (4 points)

1. Donner la syntaxe micro-C pour déclarer un symbole fonctionnel `abs` tel que `abs(x)` représente la valeur absolue d'un entier `x`.

2. La valeur absolue d'un entier x (notée $|x|$ en mathématiques) est égale à x si x est positif ou nul. Sinon, elle est égale à $-x$. Avec la notation définie dans la question 1, formaliser cette définition dans la logique de micro-C, en complétant les pointillés dans la définition suivante :

```
predicate def1(int x) = ...
```

3. De même, définir un prédicat micro-C `def2` correspondant à la définition suivante : la valeur absolue d'un entier x est égale à x ou à $-x$, et c'est un entier positif ou nul.
4. Donner un code micro-C qui permet de vérifier avec l'interface en ligne que ces deux définitions sont équivalentes.

4 Puissances d'un entier, en logique de Hoare (8 points)

1. Exprimer par un triplet de Hoare que, si b est positif ou nul et si le programme

```
p := 1; i := 0; while i < b do p := a * p; i := i + 1 od
```

termine, alors il calcule a^b dans p pour tout entier a .

2. En appliquant une par une les règles de la logique de Hoare, démontrer formellement **dans un tableau** que ce triplet de Hoare est valide.
3. La déclaration

```
function int power(int a, int b);
```

introduit un symbole fonctionnel `power` d'arité 2. Reproduire et compléter les axiomes

```
axiom power0 : forall x. power(x,0) == ...;
```

```
axiom powerS : forall x. forall n. ... -> power(x,n+1) == ... power(x,n);
```

afin que `power(x,y)` formalise x^y pour tout entier x et tout entier y positif ou nul.

4. Exprimer sous forme de lemmes micro-C les propriétés $x^1 = x$ et $a^{b+c} = (a^b) * (a^c)$ pour tous les entiers b et c positifs ou nuls.

Essayez de démontrer ces deux lemmes avec l'interface en ligne de micro-C. Justifiez clairement et simplement le résultat obtenu.