Génie Logiciel Avancé

Année 2021-2022

Prof. Burkhart Wolff
wolff@lri.fr

Hugo Mlodecki, Carmelo Vaccaro
hugo.mlodecki@universite-paris-saclay.fr
carmelo.vaccaro@universite-paris-saclay.fr

TD 7 - Test structurel et Preuve de programmes

Semaine du 22 novembre 2021

Exercice 1

On considère une fonction qui prend un tableau de caractères s en argument et renvoie vrai si et seulement si un caractère a apparaît strictement plus de fois qu'un caractère b dans s.

```
boolean comp_occurrences(char s[], char a, char b) {
    int res = 0;
    int i = 0;
    while(i < s.length) {
        if(s[i] == a) { res++; }
        if(s[i] == b) { res--; }
        i++;
    }
    return (res > 0);
}
```

1. Donner une spécification formelle de `comp_occurences`. **Astuce** : En MOAL, on considère `s` comme liste de caractères, donc strings.
2. Donner le graphe de flot de contrôle de cette fonction.
3. Donner le chemin le plus court permettant de satisfaire le critère « toutes les instructions ». On notera ce chemin ch1.
4. En détaillant l'exécution symbolique, déterminer la condition de chemin de ch1. S'il est faisable, donner un test pour ce chemin (c'est-à-dire des valeurs concrètes pour les arguments et le résultat attendu), sinon expliquer pourquoi il n'est pas faisable.
5. Donner le plus court chemin ch2 tel que l'ensemble $\{\text{ch1}, \text{ch2}\}$ satisfasse le critère « toutes les transitions ».
6. En détaillant l'exécution symbolique, déterminer la condition de chemin de ch2. S'il est faisable, donner un test pour ce chemin, sinon expliquer pourquoi il n'est pas faisable.
7. On considère tous les chemins qui passent deux fois par la boucle tel que, au premier tour, la condition du premier *if* est vraie et la condition du deuxième *if* est fausse. Sans détailler l'exécution symbolique, donner la condition de chemin pour chacun de ces chemins, puis donner un test s'il est faisable. S'il ne l'est pas, expliquer pourquoi.
8. Expliquer en quelques lignes la forme que doit avoir un chemin du graphe de cette fonction pour être faisable.

Exercice 2
Dériver les triplets de Hoare suivants en utilisant les règles d'inférence introduites dans le cours. Rappel : toutes les variables sont des entiers.

1. $\vdash \{x \leq 0\}$ `y := x+2` $\{y \leq 2\}$
2. $\vdash \{x \leq 0\}$ `x := x-1` $\{x < 0\}$
3. $\vdash \{x \geq 0\}$ `WHILE x` $\geq$ `0 DO x := x-1` $\{x = -1\}$
4. $\vdash \{a = x \wedge b = y\}$ `a := a + b; b := a - 2*b; a := a * b` $\{a = x^2 - y^2\}$
5. $\vdash \{i = 8\}$ `WHILE i < 5 DO i := 2*i` $\{i \geq 5\}$

Exercice 3
On considère le programme `Prog` suivant :

```
IF x > y
THEN max := x
ELSE max := y
```

Quelles sont les pré et post-conditions de ce programme ? Démontrer la validité du triplet de Hoare correspondant.

Exercice 4
On considère le programme `Prog` suivant :

```
WHILE y != x DO
   x := x - 1;
   y := y - 2;
```

1. Quelles sont les pré et post-conditions de ce programme ?
2. Quel est l'invariant de la boucle ?
3. Démontrer la validité du triplet de Hoare correspondant à ce programme.
4. Donner un variant pour la boucle `WHILE`, c'est-à-dire une expression toujours positive et qui décroît strictement à chaque tour de boucle.

Exercice 5 (Bonus)
On veut prouver que le programme suivant calcule X^N pour $N \geq 0$.

```
S := 1;
P := N;
WHILE P >= 1 DO
   S := S * X;
   P := P - 1;
```

1. Écrire la spécification du programme sous forme de pré et post-conditions.
2. Quel est le triplet de Hoare à prouver ?
3. Trouver un invariant pour la boucle `WHILE`, puis donner la preuve de la deuxième partie du programme.
4. Donner la preuve de la première partie du programme `S:=1; P:=N` pour terminer la preuve du programme.
5. Donner un variant pour la boucle `WHILE`.

Calcul de Hoare

$$\frac{}{\vdash \{P\}\ \texttt{SKIP}\ \{P\}}\ skip \qquad \frac{}{\vdash \{P[x \mapsto E]\}\ \texttt{x :== } E\ \{P\}}\ assignment$$

$$\frac{\vdash \{P \wedge cond\}\ c\ \{Q\} \qquad \vdash \{P \wedge \neg cond\}\ d\ \{Q\}}{\vdash \{P\}\ \texttt{IF}\ cond\ \texttt{THEN}\ c\ \texttt{ELSE}\ d\ \{Q\}}\ ifthenelse$$

$$\frac{\vdash \{P \wedge cond\}\ c\ \{P\}}{\vdash \{P\}\ \texttt{WHILE}\ cond\ \texttt{DO}\ c\ \{P \wedge \neg cond\}}\ while$$

$$\frac{P \to P' \qquad \vdash \{P'\}\ c\ \{Q'\} \qquad Q' \to Q}{\vdash \{P\}\ c\ \{Q\}}\ consequence$$

$$\frac{}{\vdash \{false\}\ c\ \{P\}}\ falseE \qquad \frac{\vdash \{P\}\ c\ \{Q\} \qquad \vdash \{Q\}\ d\ \{R\}}{\vdash \{P\}\ c; d\ \{R\}}\ sequence$$