

Contrôle continu : preuves de programmes  
SUJET 1

On rappelle que la notation  $\text{prog}_{i \rightarrow j}$  désigne les lignes  $i$  à  $j$  (incluses) du programme  $\text{prog}$ .

## Exercice 1

On étudie le programme suivant :

1	$x \leftarrow x + y + 1$
2	$y \leftarrow x - y + 1$
3	$x \leftarrow x - y + 3$

**Question 1** En utilisant notamment la règle de Floyd, déterminez une formule  $Q$  la plus forte possible telle que le triplet  $\langle (x = u) \wedge (y = v) \rangle \text{ prog} \langle Q \rangle$  soit totalement correct.

**Question 2** Déterminez de la même façon une formule  $R$  (non triviale) telle que le triplet  $\langle \rangle \text{ prog} \langle R \rangle$  soit totalement correct.

**Question 3** On cherche une précondition  $P$  la plus faible possible telle que le triplet

$$\langle P \rangle \text{ prog} \langle (x = a) \wedge (y = b) \rangle$$

soit totalement correct. Montrez tout d'abord que le triplet

$$\langle (x - y + 3 = a) \wedge (y = b) \rangle \text{ prog}_{3 \rightarrow 3} \langle (x = a) \wedge (y = b) \rangle$$

est totalement correct, **sans utiliser la règle de Floyd**.

**Question 4** Pourquoi n'utilise-t-on pas la règle de Floyd dans la question précédente ?

**Question 5** En procédant comme à la question 3, montrez que le triplet

$$\langle (x = b - 2) \wedge (y = a - 2) \rangle \text{ prog}_{1 \rightarrow 3} \langle (x = a) \wedge (y = b) \rangle$$

est totalement correct, **sans utiliser la règle de Floyd**.

## Exercice 2

Soit le programme suivant :

1	$\text{if } (x > 0)$
2	$y \leftarrow 1/x$
3	$\text{else}$
4	$\text{if } (x < 0)$
5	$y \leftarrow -(1/x)$
6	$\text{else}$
7	$y \leftarrow 0$
8	$\text{endif}$
9	$\text{end if}$

Dans ce programme,  $x$  et  $y$  sont des variables réelles et la division  $1/x$  est supposée donner un résultat exact (c'est-à-dire que la formule  $\forall x ((x \neq 0) \Rightarrow (x(1/x) = 1))$  est une tautologie).

**Question 1** Déterminez une formule  $Q$  non triviale (non tautologique en particulier) telle que le triplet suivant soit totalement correct

$$\langle x \leq 0 \rangle \text{ prog}_{4 \rightarrow 8} \langle Q \vee ((x = 0) \wedge (y = 0)) \rangle$$

**Question 2** Montrez que le  $\langle \rangle \text{ prog} \langle ((x \neq 0) \wedge (y|x| = 1)) \vee ((x = 0) \wedge (y = 0)) \rangle$  est totalement correct.

### Exercice 3

On étudie le programme suivant :

	prog
1	y ← x
2	u ← 1
3	r ← 0
4	while(y >= 2)
5	r ← r + u*(y mod 2)
6	u ← 2*u
7	y ← y div 2
8	end while

Dans ce programme, toutes les variables sont des entiers de  $\mathbb{Z}$ . L'opérateur  $*$  désigne la multiplication dans  $\mathbb{Z}$ , L'opération `mod` donne le reste de la division euclidienne alors que `div` donne le quotient. La formule suivante est une tautologie

$$\forall z \in \mathbb{Z} (z = 2(z \text{ div } 2) + (z \text{ mod } 2)).$$

On pourra aussi utiliser la tautologie suivante :

$$\forall z \in \mathbb{Z} ((z \text{ mod } 2) \leq 1) \wedge ((z \text{ mod } 2) \geq 0).$$

**Question 1** Soit  $F$  la formule logique  $(uy + r = x) \wedge (y \geq 1)$ . Déterminez une précondition  $P$  telle que le triplet  $\langle P \rangle \text{ prog}_{1 \rightarrow 3} \langle F \rangle$  soit totalement correct.

**Question 2** Montrez que le triplet suivant est totalement correct

$$\langle F \wedge (y \geq 2) \rangle \text{ prog}_{5 \rightarrow 6} \langle (uy + 2r = 2x + u(y \text{ mod } 2)) \wedge (y \geq 2) \rangle.$$

**Question 3** Montrez que le triplet suivant est totalement correct

$$\langle (uy + 2r = 2x + u(y \text{ mod } 2)) \wedge (y \geq 2) \rangle \text{ prog}_{7 \rightarrow 7} \langle F \rangle.$$

La preuve nécessite l'utilisation de la tautologie donnée ci-dessus.

**Question 4** Déterminez  $Q$  telle que le triplet  $\{F\} \text{ prog}_{4 \rightarrow 8} \{Q\}$  soit *partiellement* correct. Quelles sont les valeurs possibles pour  $y$  quand  $Q$  est vraie ?

**Question 5** Proposez un *variant* pour la boucle `prog4→8` et déterminez  $R$  telle que le triplet  $\langle R \rangle \text{ prog}_{4 \rightarrow 8} \langle Q \rangle$  soit *totalement* correct avec la même post-condition  $Q$  qu'à la question précédente.

**Question 6** Déterminez  $S$  telle que le triplet  $\langle S \rangle \text{ prog } \langle Q \rangle$  soit *totalelement* correct (toujours avec la même post-condition).

**Question 7** Expliquez brièvement comment on pourrait montrer qu'à la fin du programme,  $u$  contient une puissance de 2.