

TD n°7 - Correction

Logique de Hoare

Exercice 1 Dire, dans chacun des cas suivants, si l'affectation satisfait la formule de Hoare.

1. $[x \mapsto 0] \models \{x = 0\} y := x + 1 \{y = 1\}$
2. $[x \mapsto 1] \models \{x = 0\} y := x + 1 \{y = 1\}$
3. $[x \mapsto 0] \models \{x = 0\} y := x + 1 \{y = 0\}$
4. $[x \mapsto 1] \models \{x = 0\} y := x + 1 \{y = 0\}$
5. $[y \mapsto 0] \models \{x = 1\} y := x + 1 \{y = 42\}$
6. $[x \mapsto 0, y \mapsto 1] \models \{x < 2\} y := x; x := 2; z := x * y \{z \leq 2\}$
7. $[x \mapsto 5, y \mapsto 4] \models \{y > 0\} \text{ while } 1 > 0 \text{ do } x := x + y; y := y + 1 \text{ od } \{x < 0\}$

Correction :

1. Oui.
2. Oui, car la prémisse est fausse.
3. Non, car la prémisse est vraie et la conclusion est fausse.
4. Oui, car la prémisse est fausse.
5. Oui, car la prémisse est fausse.
6. Oui, il faut exécuter le programme pour le voir.
7. Oui, car le programme ne se termine pas.

Exercice 2 Dire, dans chacun des cas suivants, si la formule de Hoare est valide, satisfaisable ou non satisfaisable.

1. $\{x < 2\} y := x; x := 2; z := x * y \{z \leq 2\}$
2. $\{x > 0\} x := 0; y := 1; \text{if } x > y \text{ then } z := y \text{ else } z := x \text{ fi } \{z > 0\}$
3. $\{(x > 0) \wedge (y > 0)\} \text{ while } 1 > 0 \text{ do } x := x + y; y := y + 1 \text{ od } \{x < 0\}$
4. $\{(y > 0) \wedge (z = y)\} x := 0; \text{while } z > 0 \text{ do } x := x + z; z := z - 1 \text{ od } \{2 * x = (y * (y + 1))\}$

Correction :

1. Valide, car la valeur de z est le double de la valeur initiale de x
2. Pas valide : il suffit de prendre une affectation qui satisfait la précondition, la valeur finale de z est 0. La formule est satisfaisable, elle est satisfaite par toute affectation qui ne satisfait *pas* la précondition.
3. Valide, car pour toute affectation initiale le programme ne se termine pas (il boucle).
4. Valide, c'est la formule de Gauss.

Exercice 3 Est-ce que la formule de Hoare :

$$\{\text{True}\} x := e \{x = e\}$$

est valide pour toute expression e ?

Correction : D'après la Définition 26, la formule de Hoare est valide si et seulement si pour toute affectation σ on a $\sigma(e) = \sigma'(e)$ avec $\sigma' = \sigma[x/\sigma(e)]$.

Cela est toujours le cas si x n'apparaît pas dans e (car σ et σ' ne diffèrent que sur x).

Mais si x apparaît dans e , cela n'est pas en général le cas (ex : $e = x + 1$), mais peut tout de même l'être pour des cas bien particuliers et peu intéressants (ex : $e = x$ ou $e = 3 * x - 2 * x$).

La formule n'est donc pas valide pour toute expression e .

Exercice 4 Dire, dans chacun des cas suivants, pour quels programmes P la formule de Hoare est valide

1. $\{\text{True}\} P \{\text{True}\}$
2. $\{\text{False}\} P \{\text{False}\}$
3. $\{\text{False}\} P \{\text{True}\}$
4. $\{\text{True}\} P \{\text{False}\}$

Correction : Toute formule de Hoare dont la pré-condition est **False** ou dont la post-condition est **True** est valide quel que soit le programme.

1. Tout programme, car il y a **True** comme post-condition
2. Tout programme, car il y a **False** comme pré-condition
3. Tout programme, car il y a **False** comme pré-condition
4. Les programmes qui ne se terminent jamais (divergent).

Exercice 5 Trouvez une expression booléenne f qui rend valides les formules suivantes. Cherchez la formule f la plus "simple" (dans quel sens ?)

1. $\{f\} x := x + 2 \{x = 5\}$
2. $\{f\} x := y \{x = y\}$
3. $\{f\} y := 1; \text{while } y > 0 \text{ do } y := y + x \text{ od } \{y = 2\}$
4. $\{x > 2\} x := x + 2 \{f\}$
5. $\{x > 0 \vee x < -1\} \text{if } x > 0 \text{ then } x := x + 1 \text{ else } x = -x \text{ fi } \{f\}$

Correction :

1. $x = 3$
2. $y = y$
3. $x \geq 0$: Si le programme termine on a que $y \leq 0$, et la postcondition n'est pas satisfaite. Il faut donc assurer que le programme ne termine pas.
4. $x > 4$
5. $x > 1$