Travaux Dirigés No6
Logique de Hoare I

Frédéric Peschanski

1er mars 2017

Dans ce TD nous effectuons nos premières preuves en logique de Hoare.

Exercice 1 : Recherche de la plus faible précondition

Question 1 : Affectations

Chercher la plus faible précondition P qui satisfait :

— $\{P\}$ i = i + 1 $\{i > 0\}$
— $\{P\}$ k = (lo+hi) div 2 $\{lo \leq k \leq hi\}$

Question 2 : Séquencement

Chercher la plus faible précondition P qui satisfait :

— $\{P\}$ x = x - 1 ; y = y - 1 $\{x = y\}$
— $\{P\}$ y = x ; u = 4 * x + 3 * y ; t = 3 * x + 5 * y $\{t = 8 \wedge u = 7\}$

Question 3 : Alternative

Chercher la plus faible précondition P qui satisfait :

— $\{P\}$ **if** (x > 0) z = x **else** z = - x $\{z = |x|\}$
— $\{P\}$ x = 4 ; **if** (x > y) z = x **else** z = y $\{z = 3\}$

Exercice 2 : Preuve de programme

Question

Démontrer les triplets de Hoare suivants :

— $\{x > 2\}$ a = 1 ; y = x ; y = y - a $\{y > 0 \wedge x > y\}$
— $\{i > 0\}$ **if** (i == 0) j = 0 **else** j = 1 $\{j = 1\}$

Exercice 3 : Des contrats aux preuves

On suppose que le code Java suivant résulte d'une démarche de conception par contrat.

```
public class Flips {
    // attributs = observateurs
    private int x, y, z;

    public Flips(int x, int z) { this.x = x; this.y = x; this.z = z; }

    public checkInvariant() { assert((x <= y) && (y <= z)); }

    public void flip(boolean flag) {
        // PRE
        assert(y < z)

        // PRE_INV
        checkInvariant();

        // CAPTURES
        int Y_PRE = y

        if(flag) {
            if(y == x) {
                y = z;
            } else {
                y = x;
            }
        } else {
            y = y + 1;
        }

        // POST_INV
        checkInvariant();

        // POST
        assert( y != Y_PRE );
    }
}
```

Question 1

Donner les *obligations de preuve* pour démontrer la correction du corps de la méthode `flip()`.

Question 2

Résoudre les obligations de preuve en logique de Hoare. En cas de "blocage" proposez des correctifs pour la postcondition et/ou l'invariant.

Annexe : Règles de la logique de Hoare (première partie)

$$\frac{}{\{Q[expr/V]\}\texttt{V} = \texttt{expr}\{Q\}}\,(\text{aff})$$

$$\frac{\{P\}\texttt{I}_1\{Q_1\} \quad \{Q_1\}\texttt{I}_2\{Q_2\} \quad \ldots \quad \{Q_{n-1}\}\texttt{I}_\texttt{n}\{R\}}{\{P\}\texttt{I}_1;\texttt{I}_2;\ldots;\texttt{I}_\texttt{n}\{R\}}\,(\text{seq})$$

$$\frac{P \implies P' \quad \{P'\}C\{Q\}}{\{P\}C\{Q\}}\,(mp-pre)$$

$$\frac{\{P_1\}\texttt{C}_1\{Q\} \quad \{P_2\}\texttt{C2}\{Q\}}{\{(B \implies P_1) \wedge (\neg B \implies P_2)\}\texttt{if (B) C}_1\texttt{; else C2}\{Q\}}\,(\text{alt})$$