TD de Méthodes formelles

Sémantique

Exercice 1. *Soit le programme suivant :*

```
q := 0; x := a;
while   b <= x   do
  x := x + - b;
  q := q + 1;
  r := a + - (q * b);
done
```

1. *Calculer sa sémantique opérationnelle à grand pas dans l'environnement* $\{\mathsf{a} \mapsto 11, \mathsf{b} \mapsto 6\}$
2. *Définir le graphe de contrôle du programme, et donner la trace de l'exécution en partant de l'environnement* $\{\mathsf{a} \mapsto 11, \mathsf{b} \mapsto 6\}$

Exercice 2. *Les triplets de Hoare suivants sont-ils valides ?*

- $\{\mathsf{x} = 10\}\mathsf{x} := \mathsf{x} + 1\{\mathsf{x} = 11\}$ *?*
- $\{\mathsf{c} = 0\}$if c then x = c else x = 1 fi$\{\mathsf{x} = 0 \wedge \mathsf{c} = 0\}$ *?*
- $\{\mathsf{c} = 2\}$if c then x = c else x = 1 fi$\{\mathsf{x} = 2 \wedge \mathsf{c} = 2\}$ *?*
- $\{faux\}\mathsf{x} = 0; \mathsf{y} = 1\{\mathsf{x} = 0 \wedge \mathsf{y} = 2\}$ *?*
- $\{\mathsf{i} = 1\}$while i <= 10 do i := i + 1 done$\{\mathsf{i} = 10\}$ *?*
- $\{\mathsf{i} = 1\}$while ! (i <= 0) do i := i + 1 done$\{\mathsf{i} = 0\}$ *?*

Exercice 3. *Démontrer la validité des triplets de Hoare suivants.*

1. $\{\}$
   if c then $i := 0; x := i$ else $x := c$ fi
   $\{x = 0\}$
2. $\{\}$
   $N := 10; sum := 0; i := 1;$
   while i <= N do $sum := sum + i; i := i + 1$ done
   $\{sum = 55\}$

   rappel : $\sum_{i=1}^{n} i = n \times (n+1)/2$

Spécification

Exercice 4. *Spécifiez par des préconditions / postconditions les fonctions suivantes :*

```
// returns the absolute value of x
int abs(int x) {
  if (x >= 0)
    return x;
  return -x;
}


// return the max value between x and y
int max(int x, int y) {
  if (x >= y)
    return x;
  return y;
}


// return the max value between *p and *q
int max_ptr(int *p, int *q) {
  if (*p >= *q)
    return *p;
  return *q;
}


// -1 if elt not in a, index where to find elt otherwise
int find(int* a, int length,int elt) {...}
```

Calcul de WP

Exercice 5. *À l'aide d'un calcul de plus faible précondition, indiquer si les propriétés Q sont valides ou non après l'exécution des programmes suivants.*

1. $Q : x = 0$

   programme :
   if c then $i := 0; x := i$ else $x := c$ fi

2. $Q : sum = 55$

   programme :
   $N := 10; sum := 0; i := 1;$
   while $i <= N$ do $sum := sum + i; i := i + 1$ done
   rappel : $\sum_{i=1}^{n} i = n \times (n+1)/2$

Analyse dataflow

Exercice 6.

1. *Définir l'opération abstraite* $\times^\sharp$ *sur le domaine des intervalles* $(Interv, \sqsubseteq)$.
2. *Définir la fonction de transition abstraite dans le cas de l'étiquette* ?e *sur* $(Interv, \sqsubseteq)$.
3. *Soit le programme*

   ```
   if x > 100 then x:=100 fi;
   if x < 0 then x:=0 fi;
   s:=0;
   y:=1;
   while y <= x do s:=s+y; y:= y+1; done
   ```

   Quel est l'environnement abstrait résultant de l'exécution de ce programme pour le domaine des intervalles ?

Exercice 7. *Définir des domaines pour les analyses suivantes (éléments abstraits,* $\sqcup$, $\sqcap$, $\sqsubseteq$, *transition abstraite) :*

1. *Analyse de teinte. On supposera notamment que la fonction* `int input()` *retourne un entier teinté, que la fonction* `int sanitize(int x)` *déteinte un entier et que la fonction* `vulnerable-fun(int x)` *émet une erreur si* `x` *est teinté.*
2. *Analyse de nullité des pointeurs (*`malloc` *retourne un pointeur pouvant être nul,* `*x` *échoue si le pointeur est nul)*
3. *Analyse de définition de variable*
4. *Domaine d'égalité entre variables*