Variant et invariant de boucle

Renaud Costadoat
Lycée Dorian

Table des matières

Problématique

Objectif

L'objectif de ce cours et de savoir:

- justifier qu'une boucle produit l'effet attendu au moyen d'un invariant,
- démontrer qu'une boucle se termine effectivement.

Algorithme 1 : Calcul de k^n

Entrées: entier n, réel k

Sorties: réel puissance

```
c=n
puissance=1
tant que c>0 faire
        puissance=puissance*k
        c=c-1
retourner puissance
```

Cet algorithme permet de calculer la $n^{ème}$ puissance de k.

Pour terminer cet algorithme, la variable *c* est calculée à chaque itération, puis testée.

Ainsi, lorsqu'elle atteint une certaine valeur, la boucle s'arrête.

Comment prouver que cette boucle s'arrête ?

Variant de boucle

Definition

Soit une condition booléenne permettant de sortir d'une boucle constituée d'une comparaison entre une variable et une constante de types entiers positifs. La variable est un **variant de boucle** si elle est :

- entière,
- bornée,
- strictement croissante ou décroissante.

Ainsi, après un nombre fini d'itérations, on est sûr que la boucle se terminera.

Remarque

- Un variant de boucle permet de s'assurer qu'une boucle se terminera,
- Un variant de boucle ne permet pas de s'assurer qu'un algorithme fournit la réponse attendue.

Exemple de variant de boucle

Objectif: Montrer que l'algorithme 1 s'arrête.

Dans la boucle, c est définie par la suite $\{c_i\}$ telle que, dans la boucle :

$$\begin{cases} c_0 = n \\ c_{i+1} = c_i - 1 \rightarrow \forall i, c_{i+1} < c_i \\ \forall i, c_i > 0 \end{cases}$$

La suite $\{c_i\}$ est entière, positive et strictement décroissante.

Cela permet de justifier que l'algorithme s'arrête et c est un variant de boucle.

Table des matières

Invariant de boucle

Definition

Dans le cas des *structures itératives*, un **invariant de boucle** est une propriété ou une formule logique:

- qui est vérifiée après la phase d'initialisation,
- qui reste vraie après l'exécution d'une itération,
- qui, conjointement à la condition d'arrêt, permet de montrer que le résultat attendu est bien le résultat calculé.

1. Définir les préconditions (état des variables avant d'entrer dans la boucle).
2. Définir un invariant de boucle.
3. Prouver que l'invariant de boucle est vrai.
4. Montrer la terminaison du programme.
5. Montrer qu'en sortie de boucle, la condition reste vraie.

Exemple d'invariant de boucle

Objectif: Montrer que l'algorithme donne le résultat attendu.

Dans la boucle, deux suites $\{p_i\}$ (puissance) et $\{c_i\}$ sont définies par récurrence :

$$\begin{cases} p_0 = 1 & p_{i+1} = k * p_i \\ c_0 = n & c_{i+1} = c_i - 1 \end{cases}$$

On veut montrer qu'en sortie de la boucle $p = k^n$.

Hypothèse: $P_i : p_i = k^{n-c_i}$ est un invariant de boucle.

- $P_0 : p_0 = k^{n-c_0} = k^{n-n} = 1$, VRAI,
- Hypothèse: $P_i : p_i = k^{n-c_i}$,
- $P_{i+1} : p_{i+1} = k * p_i = k * k^{n-c_i} = k^{n-(c_i-1)} = k^{n-c_{i+1}}$, VRAI.

P_i **est un invariant de boucle et le résultat est le bon:** $p = k^n$**.**

Exemple d'algorithme du PGCD sous python

Objectif: Coder sous python cet algorithme.

Data : a,b $\in \mathbb{N}^*$

x $\leftarrow$ a

y $\leftarrow$ b

tant que $y \neq 0$ faire

r $\leftarrow$ reste de la division euclidienne de x par y

x $\leftarrow$ y

y $\leftarrow$ r

fin

Afficher x

```
x=a
y=b
while y!=0:
    r=x%y
    x=y
    y=r
print x
```

Application au PGCD: Variant de boucle

Déterminer le variant de boucle et montrer que la boucle se termine.

Data : a,b $\in \mathbb{N}^*$

x $\leftarrow$ a

y $\leftarrow$ b

tant que $y \neq 0$ faire

  r $\leftarrow$ reste de la division euclidienne de x par y

  x $\leftarrow$ y

  y $\leftarrow$ r

fin

Afficher x

Par définition:

- Le reste de la division euclidienne de x par y, r, est un entier positif strictement inférieur à y,
- A chaque itération, y prend la valeur de r.

$\rightarrow$ Donc, y décroit à chaque itération.

$\rightarrow$ y **est un variant de boucle**.

Application au PGCD: Invariant de boucle

Montrer que $x_n = r_n + y_n.q_n$ est un invariant de boucle et que la boucle donne le résultat attendu.

Data : a,b $\in \mathbb{N}^*$
x $\leftarrow$ a
y $\leftarrow$ b
tant que $y \neq 0$ faire
 r $\leftarrow$ reste de la division euclidienne de x par y
 x $\leftarrow$ y
 y $\leftarrow$ r
fin
Afficher x

- Initialement $x_0 = a$ et $y_0 = b$,
- On postule que l'invariant est x, or: $x = q.y + r \Leftrightarrow r = x - q.y$,
- Il existe un r_1 tel que $r_1 = x_1 - q_1.y_1$,
- Hypothèse $r_n = x_n - q_n.y_n$,
- Il existe $r_{n+1} = x_{n+1} - q_{n+1}.y_{n+1}$, avec $x_{n+1} = y_n$ et $y_{n+1} = r_n$,
- On a déjà montré que la boucle s'arrête avec $y = 0$,
- En sortant de la boucle on a bien $x = r$,
- x **est donc l'invariant de boucle**.