Cartouche du document

Année : ING 1
Matière : Algorithmique I
Activité : Travail dirigé

Objectifs

L'objectif de cette série d'exercice est

- * d'effectuer des rappels sur la syntaxe que nous allons utiliser tout au long du semestre en algorithmique
- * de présenter les invariants de boucle (vérification formelle)
- * d'introduire la notion de coût d'un algorithme (complexité)

Sommaire des exercices

Corps des exercices

1 - Calcul du pgcd de deux entiers

Question 1)

Énoncé de la question

Ecrire une fonction qui calcule le pgcd de deux entiers passés en paramètres.

Solution de la question

```
fonction pgcd(a : Entier, b : Entier) : Entier
variables
        a1, b1 : Entier
Début
        r <-- a mod b
        a1 <-- a
        b1 <-- b
        Tantque r > 0 Faire
                a1 <-- b1
                b1 <-- r
                r <-- a1 mod b1
        Fin Tantque
        retourner b1
Fin
```

Question 2)

Énoncé de la question

Trouver un invariant de boucle pour votre fonction pgcd et démontrer la validité du résultat.

Solution de la question

Tout d'abord démontrons le résultat suivant :

a = b * q + r et r > 0 ==> pgcd(a,b) = pgcd(b,r)

preuve :
q' un diviseur de a et b ==> a = k1 * q' et b = k2 * q'
r = a - b * q ==> r = q' * (k1 - k2 q) et (k1 - k2 q) ≠ 0
r = q' * (k1 - k2 q) et (k1 - k2 q) ≠ 0 ==> q' est un diviseur de r
Conclusion : r 0 et q' un diviseur de a et b ==> q' est un diviseur de r

soit q' un diviseur de b et r alors r = k1 * q' et b = k2 * q'
a = b * q + r ==> a = q' * (k2 * q + k1) et (k2 * q + k1) ≠ 0
a = q' * (k2 * q + k1) et (k2 * q + k1) ≠ 0 ==> q' est un diviseur de a
Conclusion : r > 0 et q' un diviseur de a et r ==> q' est un diviseur de a

On en déduit {d ∈ N / a = q1 * d et b = q2 * d } = {d ∈ N / b = q2 * d et r = q3 * d }
donc a = b * q + r et r > 0 <==> pgcd(a,b) = pgcd(b,r)
Fin de la preuvez

On note p le pgcd de a et b et on définit l'invariant de boucle suivant :

{ p = pgcd(a1,b1) et r = a1 mod b1 }

Insérons l'invariant de boucle dans l'algorithme.

```
fonction pgcd(a : Entier, b : Entier) : Entier
variables
        a1, b1 : Entier
Début
 r <-- a mod b
 a1 <-- a
 b1 <-- b
 // Dans la première instruction, on a affecté à r
 // la valeur a1 mod b1
 // a1 vaut a et b1 vaut b ==> p = pgcd(a1,b1)
 // On en déduit l'invariant
 { p = pgcd(a1,b1) et r = a1 mod b1 }
 Tantque r > 0 Faire
  // Par construction de l'invariant de boucle,
  // l'invariant est vrai en début d'itération
  { p = pgcd(a1,b1) et r = a1 mod b1 }
  a1 <-- b1
```

```
  b1 <-- r
  r <-- a1 mod b1
  // On note a1' l'ancienne valeur de a1, b1' l'ancienne valeur de
b1
  // de même on note r' l'ancienne valeur de r
  // D'après le théorème démontré ci-dessus, on a p =
pgcd(a1',b1') = pgcd(a1,b1)
  // de plus la dernière instruction donne r = a1 mod b1
  // On en déduit l'invariant
  { p = pgcd(a1,b1) et r = a1 mod b1 }
 Fin Tantque
 { p = pgcd(a1,b1) et r = a1 mod b1 } et r = 0
 // On en déduit b1 = p = pgcd(a,b)
 retourner b1
Fin
```