Multiplication Russe

ADOLPHE Benjamin-BERJOLA Matthias

30 avril 2020

CHAPITRE 1

Introduction

Dans le cadre de l'UE calculabilité et complexité nous avons dû réaliser plusieurs tâches sur un algorithme comprenant un contrat pré-conditions/post-conditions clair, et incluant au moins une boucle tant-que.Nous avons choisis de travailler sur l'algorithme représentant la multiplication russe et d'effectuer les tâches suivantes sur ce dernier :

- Écrire son code Dafny
- Montrer la correction totale :
  - Montrer la correction partielle : les invariants seront présentées et prouvés, ainsi que les post-conditions.
  - Prouver sa terminaison : fonctions de rang et éventuels invariants seront présentées et prouvés
- Déterminer sa complexité en temps qui dans le pire des cas sera justifiée et possiblement validée expérimentalement

  Nous allons donc exposé nos travaux dans ce rapport en prenant soin de suivre l'ordre décrit ci-dessus

CHAPITRE 2

Code en Dafny

```
1   method mulitplicationRusse(x:nat,y:nat) returns (m:nat)
2   ensures m==x*y{
3       var a := x;
4       var b := y;
5       var r := 0;
6       while(a>0)
7           invariant a>=0
8           invariant r+a*b == x*y
9           decreases a
10      {
11          if(a%2 == 0){
12              b:=2*b;
13              a:=a/2;
14          }else{
15              r:=r+b;
16              a:=a-1;
17          }
18      }
19      m:=r;
20  }
```

Algorithme 12 : multiplication russe

Entrées : x et y, deux entiers naturels
Sorties : un entier
a : *entier* $\leftarrow x$
b : *entier* $\leftarrow y$
r : *entier* $\leftarrow 0$
(*) **tant que** $a > 0$ **faire**
  si $a\%\ 2 = 0$ **alors**
    $b \leftarrow 2 * b$
    $a \leftarrow a//2$
  sinon
    $r \leftarrow r + b$
    $a \leftarrow a - 1$
  fin
fin
retourner r

CHAPITRE 3

Correction totale

3.1 Correction partielle

Méthode de détermination de la correction partielle

On commence par déterminer l'invariant de boucle en posant les cas de base et de récursivité.

Invariant en (*) $a \geq 0$:

- Cas Inductif : x est affecté à a or x est un entier naturel ainsi par typage $a \geq 0$.
- Cas Récursif : nous supposons que l'invariant $a \geq 0$ est vrai, montrons alors $a' \geq 0$:
  - 1er cas : est pair. Nous savons que $\forall(a, a', b, b', r, r') \in \mathbb{N}^6 \begin{bmatrix} (a \geq 0 \wedge a > 0 \wedge \\ a' = (\frac{a}{2}) \wedge a\%2 = 0 \wedge \\ b' = 2 * b \wedge r' = r) \end{bmatrix}$.
    Ainsi nous avons $a \geq 0 \Leftrightarrow \frac{a}{2} \geq \frac{0}{2} \Leftrightarrow a' \geq 0$.
  - 2ème cas : a est impair. Nous savons que $\forall(a, a', b, b', r, r') \in \mathbb{N}^6$ $\begin{bmatrix} (a \geq 0 \wedge a > 0 \wedge \\ r' = r + b \wedge b' = b \wedge \\ a' = a + 1 \wedge a\%2 = 1 \end{bmatrix}$. Ainsi nous avons $a \geq 0$ d'après le test de boucle or $a \geq 0 \Leftrightarrow a - 1 \geq 0 - 1 \Leftrightarrow a' \geq 0$.

Conslusion

Dans les deux cas, nous avons bien montré que $a' \geq 0$. $a \geq 0$ est donc bien un invariant de boucle en $(*)$.

Invariant $(*) r + a * b = x * y$:

- Cas Inductif : 0 est affecté à r, x est affecté à a et y est affecté à b ainsi $r + a * b = 0 + a * b = x * y$. On a donc bien $r + a * b = x * y$.
- Cas Récursif : nous supposons que l'invariant $r + a * b = x * y$ est vrai, montrons alors que $r' + a' * b' = x' * y'$ est vrai :

- 1er cas : a est pair. Nous savons que $\forall(a, a', b, b', r, r', x, x', y, y') \in \mathbb{N}^{10}$
$\left[\begin{array}{c} r + a * b = x * y \wedge a > 0 \wedge \\ a\%2 = 0 \wedge a' = \frac{a}{2} \wedge r' = r \wedge \\ b' = 2 * b \wedge x' = x \wedge y' = y \end{array}\right]$.
Ainsi nous avons $r' + a' * b' = r' + \frac{a}{2} * 2 * b = r + a * b$ or d'après invariant $r + a * b = x * y$ et $x * y = x' * y'$. Nous avons donc bien $r' + a' * b' = x' * y'$.
- 2ème cas : a est impair. Nous savons que $\forall(a, a', b, b', r, r', x, x', y, y') \in \mathbb{N}^{10}$
$\left[\begin{array}{c} r + a * b = x * y \wedge a > 0 \wedge \\ a\%2 = 1 \wedge a' = a - 1 \wedge b' = b \wedge \\ r' = r + b \wedge b' = b \wedge x' = x \wedge y' = y \end{array}\right]$.
Ainsi nous avons $r' + a' * b' = r + b + (a - 1) * b = r + a * b + b - b = r + a * b$ or d'après l'invariant nous avons $r + a * b = x * y$et $x * y = x' * y'$. Nous avons donc bien $r' + a' * b' = x' * y'$.

Conclusion

Dans les deux cas, nous avons montré que $r' + a' * b' = x' * y'$. $r + a * b = x * y$ est donc un invariant de boucle en $(*)$.

3.2 Terminaison

Méthode de détermination de la terminaison

On détermine une fonction de rang et on prouve que celle-ci est valide. C'est-à-dire, on vérifie que la fonction de rang $\in \mathbb{R}$ au point T1 et qu'elle décroit lorsque l'exécution passe entre les points T1 et T2.

Fonction de rang à valeur dans $\mathbb{N}$:

— À chaque passage au point T1, montrons que $a \in \mathbb{N}$. D'après l'invariant de boucle $a \geq 0$ nous savons donc que $a \in \mathbb{N}$.

— À chaque fois que l'exécution passe entre le point T1 et le point T2, montrons que a décroit strictement.

- 1er cas : a est pair.Nous savons que $\forall(a, a', b, b', r, r', x, x', y, y') \in \mathbb{N}^{10}$
$\left[\begin{array}{c} r + a * b = x * y \wedge a > 0 \wedge \\ a\%2 = 0 \wedge a' = \frac{a}{2} \wedge r' = r \wedge \\ b' = 2 * b \wedge x' = x \wedge y' = y \end{array}\right]$. Ainsi nous avons $a' = \frac{a}{2}$ donc $a > \frac{a}{2} \Leftrightarrow a > a'$.
Nous avons bien a strictement décroissante.
- 2ème cas : a est impair. Nous savons que $\forall(a, a', b, b', r, r', x, x', y, y') \in \mathbb{N}^{10}$
$\left[\begin{array}{c} r + a * b = x * y \wedge a > 0 \wedge \\ a\%2 = 1 \wedge a' = a - 1 \wedge b' = b \wedge \\ r' = r + b \wedge b' = b \wedge x' = x \wedge y' = y \end{array}\right]$. Ainsi nous avons $a' = a - 1$ donc $a > a - 1 \Leftrightarrow a > a'$. Nous avons bien a strictement décroissante.

Conclusion

Dans les deux cas, nous avons montré que a est strictement décroissante. a est donc une fonction de rang à valeur dans $\mathbb{N}$.

CHAPITRE 4

Complexité