Multiplication Russe

ADOLPHE Benjamin-BERJOLA Matthias

30 avril 2020

CHAPITRE 1

Introduction

Dans le cadre de l'UE calculabilité et complexité nous avions 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 suivante sur ce dernier :

- Écrire son code Dafny
- Prouver sa terminaison : fonctions de rang et éventuels invariants seront présentées et prouvés
- Montrer la correction partielle : les invariants seront présentées et prouvés, ainsi que les post-conditions.
- 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

```
method mulitplicationRusse(x:nat,y:nat) returns (m:nat)
ensures m==x*y{
    var a := x;
    var b := y;
    var r := 0;
    while(a>0)
        invariant a>=0
        invariant r+a*b == x*y
        decreases a
    {
        if(a%2 == 0){
            b:=2*b;
            a:=a/2;
        }else{
            r:=r+b;
            a:=a-1;
        }
    }
    m:=r;
}
```

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

Terminaison

Méthode de détermination de la terminaison

On commence par déterminer l'invariant de boucle en posant les cas de base et de récursivité.On détermine ensuite une fonction de rang et on prouve que celle-ci est valide.

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 $\begin{bmatrix} (a \geq 0 \wedge a > 0 \wedge \\ a' = (\frac{a}{2}) \wedge a\%2 = 0 \wedge \\ b' = 2 * b \wedge r' = r) \end{bmatrix}$.
Ainsi nous avons $a \geq 0 \Leftrightarrow \frac{a}{2} \geq \frac{0}{2} \Leftrightarrow a' \geq 0$.
Conclusion : Dans les deux cas, nous avons bien montré que $a' \geq 0$

2ème cas : a est impair : Nous savons que $\begin{bmatrix} (a \geq 0 \wedge a > 0 \wedge \\ r' = r + b \wedge b' = b \wedge \\ a' = a + 1 \wedge a\%2 = 1 \end{bmatrix}$.

Conslusion

Ainsi nous avons $a \geq 0$ d'après le test de boucle or $a \geq 0 \Leftrightarrow a - 1 \geq 0 - 1 \Leftrightarrow a' \geq 0$.

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 $\begin{bmatrix} (r + a * b = x * y \wedge a > 0 \wedge \\ a\%2 = 0 \wedge a' = \frac{a}{2} \wedge r' = r \wedge \\ b' = 2 * b \wedge x' = x \wedge y' = y \end{bmatrix}$

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 $\begin{bmatrix} (r + a * b = x * y \wedge a > 0 \wedge \\ a\%2 = 1 \wedge a' = a - 1 \wedge b' = b \wedge \\ r' = r + b \wedge b' = b \wedge x' = x \wedge y' = y \end{bmatrix}$

Conclusion

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 $r' + a' * b' = x' * y'$

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 $(*)$.

CHAPITRE 4

Correction partielle

CHAPITRE 5

Complexité