

## GCL: EJEMPLO DE VERIFICACIÓN

Rodrigo Cardoso  
Enero de 2001

La verificación de ciclos se adelanta de acuerdo con la regla de corrección correspondiente. Esta afirma que, para mostrar la corrección de un ciclo

```
{Q}
INIC;
{inv P}
{cota t}
do BB  $\rightarrow$  IF od
{R}
```

basta chequear las afirmaciones:

- 1 P vale antes, i.e.,  $\{Q\} \text{ INIC } \{P\}$
- 2 P sirve, i.e.,  $P \wedge \neg BB \Rightarrow R$
- 3 P invariante, i.e.,  $\{P \wedge BB\} \text{ IF } \{P\}$
- 4 Hay terminación, i.e.,  $\{P \wedge BB \wedge t=t_0\} \text{ IF } \{t < t_0\}$

Cuando se trata de ciclos de más de una forma de iterar, las condiciones 3 y 4 deben valer en cada caso posible. Es decir, en cada caso posible el invariante se debe mantener y la cota debe rebajar.

### EJERCICIO 2.6.1 [CAR1993]

Verificar:

```
{Q:  $b \geq 0$ }
x, y, z := a, b, 0;
{Inv P:  $y \geq 0 \wedge z + x * y = a * b$ }
do  $y > 0 \wedge \text{par}.y \rightarrow x, y := x + x, y \div 2$ 
[]  $\neg \text{par}.y \rightarrow z, y := z + x, y - 1$ 
od
{R:  $z = a * b$ }
```

#### [1] P vale antes

```
{Q} x, y, z := a, b, 0 {P}
=  $\langle \text{Ax asgn} \rangle$ 
 $Q \Rightarrow P[x, y, z := a, b, 0]$ 
=
 $b \geq 0 \Rightarrow b \geq 0 \wedge 0 + a * b = a * b$ 
(1) (2) (3)
=  $\langle 1 \Rightarrow 2: p \Rightarrow p; 3: \text{aritmética} \rangle$ 
true
```

#### [2] P sirve

```
BB
=
 $(y > 0 \wedge \text{par}.y) \vee \neg \text{par}.y$ 
=  $\langle \text{absorción} \rangle$ 
 $y > 0 \vee \neg \text{par}.y$ 
```

Por tanto:

$$\begin{aligned}
& \neg BB \\
= & \langle \text{DeMorgan} \rangle \\
& y \leq 0 \wedge \text{par}.y \\
= & \langle y: \mathbf{nat} \rangle \\
& y=0 \\
\mathbf{Hip}: & (P, \neg BB) \ y \geq 0, \ z+x*y = a*b, \ y=0 \\
& \text{true} \\
= & \langle \text{Hip: } z+x*y = a*b \rangle \\
& z+x*y = a*b \\
= & \langle \text{Hip: } y=0; \ u+0=u \rangle \\
& z = a*b
\end{aligned}$$

### [3] P invariante

[a]

$$\begin{aligned}
& \{P \wedge y>0 \wedge \text{par}.y\} \ x, y := x+x, y \div 2 \ \{P\} \\
= & \\
& P \wedge y>0 \wedge \text{par}.y \Rightarrow P[x, y := x+x, y \div 2] \\
= & \\
& y \geq 0 \wedge z+x*y = a*b \wedge y>0 \wedge \text{par}.y \Rightarrow y \div 2 \geq 0 \wedge z+(x+x)*(y \div 2) = a*b \\
& (1) \qquad (2) \qquad (3) \qquad (4) \qquad (5) \qquad (6) \\
= & \langle 1 \Rightarrow 5: \text{propiedades de } \div \\
& \quad (4 \Rightarrow y \div 2 = y/2; \ x+x = 2*x; \text{Cancelacion-}*) \Rightarrow 6 \rangle \\
& \text{true}
\end{aligned}$$

[b]

$$\begin{aligned}
& \{P \wedge \neg \text{par}.y\} \ z, y := z+x, y-1 \ \{P\} \\
= & \\
& P \wedge \neg \text{par}.y \Rightarrow P[z, y := z+x, y-1] \\
= & \\
& y \geq 0 \wedge z+x*y = a*b \wedge \neg \text{par}.y \Rightarrow y-1 \geq 0 \wedge z+x+x*(y-1) = a*b \\
& (1) \qquad (2) \qquad (3) \qquad (4) \qquad (5) \\
= & \langle 1 \wedge 3 \Rightarrow 4: \text{aritmética}; \\
& \quad 2 \Rightarrow 5 : \text{aritmética} \rangle \\
& \text{true}
\end{aligned}$$

### [4] Terminación

Informal: la cota  $y$  disminuye efectivamente en cada caso. En el primer caso debe notarse que  $y$  es par y positivo, de modo que  $y/2 < y$ .

Formal:

[a]

$$\begin{aligned}
& \{P \wedge y>0 \wedge \text{par}.y \wedge y=y_0\} \ x, y := x+x, y \div 2 \ \{y < y_0\} \\
= & \\
& P \wedge y>0 \wedge \text{par}.y \wedge y=y_0 \Rightarrow (y < y_0)[x, y := x+x, y \div 2] \\
= & \\
& y \geq 0 \wedge z+x*y = a*b \wedge y>0 \wedge \text{par}.y \wedge y=y_0 \Rightarrow y \div 2 < y_0 \\
& (1) \qquad (2) \qquad (3) \qquad (4) \qquad (5) \qquad (6)
\end{aligned}$$

=  $\langle 3 \wedge 4 \wedge 5 \Rightarrow 6: \text{propiedades de } \div \rangle$   
true

**[b]**

$\{P \wedge \neg \text{par}.y \wedge y=y_0\} \text{ } z, y := z+x, y-1 \text{ } \{y < y_0\}$   
=  
 $P \wedge \neg \text{par}.y \wedge y=y_0 \Rightarrow (y < y_0)[z, y := z+x, y-1]$   
=  
 $y \geq 0 \wedge z+x*y = a*b \wedge \neg \text{par}.y \wedge y=y_0 \Rightarrow y-1 < y_0$   
(1)                    (2)                    (3)                    (4)                    (5)  
=  
 $\langle 4 \Rightarrow 5: \text{aritmética} \rangle$   
true