

Étude de cas 5° Preuve de programme

Calcul de la fonction puissance (bis)

1 juin 2004

Nous allons prouver que le programme

```

const int x, n;
int y;
{
  int i, z;
  i := n;
  y := 1;
  z := x;
  while (i > 0)
  {
    while (i%2 = 0)
    {
      z := z · z;
      i := i/2;
    }
    y := y · z;
    i--;
  }
}

```

calcule bien la n ième puissance du nombre entier x pour tout $n \geq 0$. (% est un symbole fonctionnel binaire qui désigne l'opération calculant le reste entier d'une division.)

Dans ce but, nous allons prouver formellement — moyennant la logique de Hoare — que y est égale à cette puissance *si le programme termine*, et ensuite nous allons prouver informellement que le programme termine effectivement. Nous allons utiliser le fait (théorème) que si $i > 0$ est pair alors $p(z, i) = p(p(z, 2), i/2) = p(z \cdot z, i/2)$ où p désigne la fonction puissance.

Preuve formelle

1	$\forall(n \in \text{int})\forall(x \in \text{int})(n \geq 0 \Rightarrow (n = 0 \Rightarrow p(x, n) = 1))$	ax def
2	$\forall(n \in \text{int})\forall(x \in \text{int})(n \geq 0 \Rightarrow (n \neq 0 \Rightarrow p(x, n) = x \cdot p(x, n - 1)))$	ax def
3	$x \in \text{int} \wedge n \in \text{int} \wedge y \in \text{int}$	hyp
4	$i \in \text{int}$	hyp
5	$z \in \text{int}$	hyp
6	$C = \text{while } (i\%2 = 0) \{z := z \cdot z; i := i/2;\} y := y \cdot z; i--;$	hyp
7	$(n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x) \Rightarrow (i \geq 0 \wedge y \cdot p(z, i) = p(x, n))$	lem 1
8	$n \geq 0 \{i := n;\} (n \geq 0 \wedge i = n)$	ax
9	$(n \geq 0 \wedge i = n) \{y := 1;\} (n \geq 0 \wedge i = n \wedge y = 1)$	ax
10	$(n \geq 0 \wedge i = n \wedge y = 1) \{z := x;\} (n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x)$	ax
11	$(n \geq 0 \wedge i = n) \{y := 1; z := x;\} (n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x)$	9, 10
12	$n \geq 0 \{i := n; y := 1; z := x;\} (n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x)$	8, 11
13	$n \geq 0 \{i := n; y := 1; z := x;\} (i \geq 0 \wedge y \cdot p(z, i) = p(x, n))$	7, 12
14	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z \cdot z, i/2) = p(x, n) \\ \wedge i\%2 = 0 \end{array} \right) \{z := z \cdot z;\} \left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i/2) = p(x, n) \\ \wedge i\%2 = 0 \end{array} \right)$	ax
15	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \\ \wedge i\%2 = 0 \end{array} \right) \{z := z \cdot z;\} \left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i/2) = p(x, n) \\ \wedge i\%2 = 0 \end{array} \right)$	14, th.
16	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \\ \wedge i\%2 = 0 \end{array} \right) \{z := z \cdot z;\} \left(\begin{array}{l} i/2 > 0 \wedge \\ y \cdot p(z, i/2) = p(x, n) \end{array} \right)$	15
17	$\left(\begin{array}{l} i/2 > 0 \wedge \\ y \cdot p(z, i/2) = p(x, n) \end{array} \right) \{i := i/2;\} \left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right)$	ax
18	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \\ \wedge i\%2 = 0 \end{array} \right) \{z := z \cdot z; i := i/2;\} \left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right)$	16, 17
19	$i > 0 \wedge y \cdot p(z, i) = p(x, n)$ $\{\text{while } (i\%2 = 0) \{z := z \cdot z; i := i/2;\}\}$ $i > 0 \wedge y \cdot p(z, i) = p(x, n) \wedge i\%2 \neq 0$	18
20	$i > 0 \wedge y \cdot p(z, i) = p(x, n)$ $\{\text{while } (i\%2 = 0) \{z := z \cdot z; i := i/2;\}\}$ $i > 0 \wedge y \cdot p(z, i) = p(x, n)$	19
21	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot z \cdot p(z, i - 1) = p(x, n) \end{array} \right) \{y := y \cdot z;\} \left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i - 1) = p(x, n) \end{array} \right)$	ax
22	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right) \{y := y \cdot z;\} \left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i - 1) = p(x, n) \end{array} \right)$	2, 21

23	$\left(\begin{array}{l} i - 1 \geq 0 \wedge \\ y \cdot p(z, i - 1) = p(x, n) \end{array} \right) \{i--;\} \left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right)$	ax
24	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i - 1) = p(x, n) \end{array} \right) \{i--;\} \left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right)$	23
25	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right) \{y := y \cdot x; i--;\} \left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right)$	22, 24
26	$\left(\begin{array}{l} i > 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right) \{C\} \left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right)$	6, 20, 25
27	$\left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \\ \wedge i > 0 \end{array} \right) \{C\} \left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right)$	26
28	$\left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right) \{\text{while } (i > 0) C\} \left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \\ \wedge i \neq 0 \end{array} \right)$	27
29	$\left(\begin{array}{l} i \geq 0 \wedge \\ y \cdot p(z, i) = p(x, n) \end{array} \right) \{\text{while } (i > 0) C\} (y = p(x, n) \wedge i \neq 0)$	28, C.S. 4°
30	$(i \geq 0 \wedge y \cdot p(z, i) = p(x, n)) \{\text{while } (i > 0) C\} y = p(x, n)$	29
31	$n \geq 0 \{i := n; y := 1; z := x; \text{while } (i > 0) C\} y = p(x, n)$	13, 30
32	$\begin{array}{l} n \geq 0 \\ \{i := n; y := 1; z := x; \\ \text{while } (i > 0) \{ \\ \text{while } (i \% 2 = 0) \{z := z \cdot z; i := i / 2;\} y := y \cdot z; i--;\} \\ y = p(x, n) \end{array}$	6, 31
33	$\begin{array}{l} n \geq 0 \\ \{i := n; y := 1; z := x; \\ \text{while } (i > 0) \{ \\ \text{while } (i \% 2 = 0) \{z := z \cdot z; i := i / 2;\} y := y \cdot z; i--;\} \\ y = p(x, n) \end{array}$	6, 32
34	$\begin{array}{l} n \geq 0 \\ \{\text{int } z; i := n; y := 1; z := x; \\ \text{while } (i > 0) \{ \\ \text{while } (i \% 2 = 0) \{z := z \cdot z; i := i / 2;\} y := y \cdot z; i--;\} \\ y = p(x, n) \end{array}$	5, 33
35	$\begin{array}{l} n \geq 0 \\ \{\text{int } i; \text{int } z; i := n; y := 1; z := x; \\ \text{while } (i > 0) \{ \\ \text{while } (i \% 2 = 0) \{z := z \cdot z; i := i / 2;\} y := y \cdot z; i--;\} \\ y = p(x, n) \end{array}$	4, 34

Commentaires

- la preuve *sous-entend* les axiomes de l'arithmétique
- l'expression *i--* est une abréviation pour l'expression $i := i - 1$
- les **invariantes** sont mises en évidence en rouge
- le programme termine parce que *i* décroît *strictement* dans les deux boucles

Lemme (1)

6.1	$n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x$	hyp
6.2	$i \geq 0$	6.1
6.3	$p(x, n) = p(x, n)$	ax
6.4	$p(x, i) = p(x, n)$	6.1, 6.3
6.5	$1 \cdot p(x, i) = p(x, n)$	6.4
6.6	$y \cdot p(x, i) = p(x, n)$	6.1, 6.5
6.7	$i \geq 0 \wedge y \cdot p(x, i) = p(x, n)$	6.2, 6.6
7	$(n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x) \Rightarrow (i \geq 0 \wedge y \cdot p(x, i) = p(x, n))$	6.1, 6.7