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 $\mathrm{p}(z,i) = \mathrm{p}(\mathrm{p}(z,2), i/2) = \mathrm{p}(z \cdot z, i/2)$ où p désigne la fonction puissance.





## Preuve formelle

| | | |
|---|---|---|
| 1 | $\forall(n \in \mathtt{int})\forall(x \in \mathtt{int})(n \geq 0 \Rightarrow (n = 0 \Rightarrow \mathrm{p}(x,n) = 1))$ | ax def |
| 2 | $\forall(n \in \mathtt{int})\forall(x \in \mathtt{int})(n \geq 0 \Rightarrow (n \neq 0 \Rightarrow \mathrm{p}(x,n) = x \cdot \mathrm{p}(x,n-1)))$ | ax def |
| 3 | $x \in \mathtt{int} \wedge n \in \mathtt{int} \wedge y \in \mathtt{int}$ | hyp |
| 4 | $i \in \mathtt{int}$ | hyp |
| 5 | $z \in \mathtt{int}$ | hyp |
| 6 | $\mathsf{C} = \mathtt{while}\ (i\%2 = 0)\ \{z := z \cdot z; i := i/2;\}\ y := y \cdot z; i\mathtt{--};$ | hyp |
| 7 | $(n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x) \Rightarrow (i \geq 0 \wedge y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n))$ | 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 | $n \geq 0\,\{i := n; y := 1; z := x;\}\,(i \geq 0 \wedge y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n))$ | 7, 12 |
| 14 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z \cdot z, i/2) = \mathrm{p}(x,n) \\ \wedge\ i\%2 = 0 \end{pmatrix}\ \{z := z \cdot z;\}\ \begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z, i/2) = \mathrm{p}(x,n) \\ \wedge\ i\%2 = 0 \end{pmatrix}$ | ax |
| 15 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n) \\ \wedge\ i\%2 = 0 \end{pmatrix}\ \{z := z \cdot z;\}\ \begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z, i/2) = \mathrm{p}(x,n) \\ \wedge\ i\%2 = 0 \end{pmatrix}$ | 14, th. |
| 16 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n) \\ \wedge\ i\%2 = 0 \end{pmatrix}\ \{z := z \cdot z;\}\ \begin{pmatrix} i/2 > 0 \wedge \\ y \cdot \mathrm{p}(z, i/2) = \mathrm{p}(x,n) \end{pmatrix}$ | 15 |
| 17 | $\begin{pmatrix} i/2 > 0 \wedge \\ y \cdot \mathrm{p}(z, i/2) = \mathrm{p}(x,n) \end{pmatrix}\ \{i := i/2;\}\ \begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n) \end{pmatrix}$ | ax |
| 18 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n) \\ \wedge\ i\%2 = 0 \end{pmatrix}\ \{z := z \cdot z; i := i/2;\}\ \begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n) \end{pmatrix}$ | 16, 17 |
| 19 | $i > 0 \wedge y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n)$<br>$\{\mathtt{while}\ (i\%2 = 0)\ \{z := z \cdot z; i := i/2;\}\}$<br>$i > 0 \wedge y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n) \wedge i\%2 \neq 0$ | 18 |
| 20 | $i > 0 \wedge y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n)$<br>$\{\mathtt{while}\ (i\%2 = 0)\ \{z := z \cdot z; i := i/2;\}\}$<br>$i > 0 \wedge y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n)$ | 19 |
| 21 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot z \cdot \mathrm{p}(z, i-1) = \mathrm{p}(x,n) \end{pmatrix}\ \{y := y \cdot z;\}\ \begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z, i-1) = \mathrm{p}(x,n) \end{pmatrix}$ | ax |
| 22 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z,i) = \mathrm{p}(x,n) \end{pmatrix}\ \{y := y \cdot z;\}\ \begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z, i-1) = \mathrm{p}(x,n) \end{pmatrix}$ | 2, 21 |

| | | |
|---|---|---|
| 23 | $\begin{pmatrix} i-1 \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i-1) = \mathrm{p}(x, n) \end{pmatrix} \{i\text{--};\} \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix}$ | ax |
| 24 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z, i-1) = \mathrm{p}(x, n) \end{pmatrix} \{i\text{--};\} \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix}$ | 23 |
| 25 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix} \{y := y \cdot x; i\text{--};\} \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix}$ | 22, 24 |
| 26 | $\begin{pmatrix} i > 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix} \{\mathsf{C}\} \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix}$ | 6, 20, 25 |
| 27 | $\begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \\ \wedge\, i > 0 \end{pmatrix} \{\mathsf{C}\} \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix}$ | 26 |
| 28 | $\begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix} \{\texttt{while}\ (i > 0)\ \mathsf{C}\} \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \\ \wedge\, i \not> 0 \end{pmatrix}$ | 27 |
| 29 | $\begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n) \end{pmatrix} \{\texttt{while}\ (i > 0)\ \mathsf{C}\} (y = \mathrm{p}(x, n) \wedge i \not> 0)$ | 28, C.S. 4° |
| 30 | $(i \geq 0 \wedge y \cdot \mathrm{p}(z, i) = \mathrm{p}(x, n)) \{\texttt{while}\ (i > 0)\ \mathsf{C}\} y = \mathrm{p}(x, n)$ | 29 |
| 31 | $n \geq 0 \{i := n; y := 1; z := x; \texttt{while}\ (i > 0)\ \mathsf{C}\} y = \mathrm{p}(x, n)$ | 13, 30 |
| 32 | $n \geq 0$<br>$\{i := n; y := 1; z := x;$<br>$\texttt{while}\ (i > 0)\ \{$<br>$\quad \texttt{while}\ (i\%2 = 0)\ \{z := z \cdot z; i := i/2;\}\ y := y \cdot z; i\text{--};\}\}$<br>$y = \mathrm{p}(x, n)$ | 6, 31 |
| 33 | $n \geq 0$<br>$\{i := n; y := 1; z := x;$<br>$\texttt{while}\ (i > 0)\ \{$<br>$\quad \texttt{while}\ (i\%2 = 0)\ \{z := z \cdot z; i := i/2;\}\ y := y \cdot z; i\text{--};\}\}$<br>$y = \mathrm{p}(x, n)$ | 6, 32 |
| 34 | $n \geq 0$<br>$\{\texttt{int}\ z; i := n; y := 1; z := x;$<br>$\texttt{while}\ (i > 0)\ \{$<br>$\quad \texttt{while}\ (i\%2 = 0)\ \{z := z \cdot z; i := i/2;\}\ y := y \cdot z; i\text{--};\}\}$<br>$y = \mathrm{p}(x, n)$ | 5, 33 |
| 35 | $n \geq 0$<br>$\{\texttt{int}\ i; \texttt{int}\ z; i := n; y := 1; z := x;$<br>$\texttt{while}\ (i > 0)\ \{$<br>$\quad \texttt{while}\ (i\%2 = 0)\ \{z := z \cdot z; i := i/2;\}\ y := y \cdot z; i\text{--};\}\}$<br>$y = \mathrm{p}(x, n)$ | 4, 34 |





## Commentaires

– la preuve *sous-entend* les axiomes de l'arithmetique
– 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 | $\mathrm{p}(x, n) = \mathrm{p}(x, n)$ | ax |
| 6.4 | $\mathrm{p}(x, i) = \mathrm{p}(x, n)$ | 6.1, 6.3 |
| 6.5 | $1 \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n)$ | 6.4 |
| 6.6 | $y \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n)$ | 6.1, 6.5 |
| 6.7 | $i \geq 0 \wedge y \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n)$ | 6.2, 6.6 |
| 7 | $(n \geq 0 \wedge i = n \wedge y = 1 \wedge z = x) \Rightarrow (i \geq 0 \wedge y \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n))$ | 6.1, 6.7 |