Étude de cas 4°

Preuve de programme

Calcul de la fonction puissance

25 mai 2004

Nous allons prouver que le programme

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

calcule bien la $n$ième puissance du nombre entier x pour tout $n \geq 0$.

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.

Preuve formelle

1	$\forall(n \in \texttt{int})\forall(x \in \texttt{int})(n \geq 0 \Rightarrow (n = 0 \Rightarrow \mathrm{p}(x,n) = 1))$	ax def
2	$\forall(n \in \texttt{int})\forall(x \in \texttt{int})(n \geq 0 \Rightarrow (n \neq 0 \Rightarrow \mathrm{p}(x,n) = x \cdot \mathrm{p}(x,n-1)))$	ax def
3	$x \in \texttt{int} \wedge n \in \texttt{int} \wedge y \in \texttt{int}$	hyp
4	$i \in \texttt{int}$	hyp
5	$\mathsf{C} = \texttt{while}\ (i > 0)\ \{y := y \cdot x; i\texttt{--};\}$	hyp
6	$(n \geq 0 \wedge i = n \wedge y = 1) \Rightarrow (i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n))$	lem 1
7	$(i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \wedge i \not> 0) \Rightarrow (y = \mathrm{p}(x,n) \wedge i \not> 0)$	lem 2
8	$(i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \wedge i > 0) \Rightarrow$ $(i \geq 0 \wedge y \cdot x \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \wedge i > 0)$	lem 3
9	$n \geq 0\,\{i := n;\}\,(n \geq 0 \wedge i = n)$	ax
10	$(n \geq 0 \wedge i = n)\,\{y := 1;\}\,(n \geq 0 \wedge i = n \wedge y = 1)$	ax
11	$n \geq 0\,\{i := n; y := 1;\}\,(n \geq 0 \wedge i = n \wedge y = 1)$	9, 10
12	$\begin{pmatrix} i \geq 0 \wedge \\ y \cdot x \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \\ \wedge\ i > 0 \end{pmatrix}\ \{y := y \cdot x;\}\ \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \\ \wedge\ i > 0 \end{pmatrix}$	ax
13	$\begin{pmatrix} i \geq 0 \wedge \\ y \cdot x \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \\ \wedge\ i > 0 \end{pmatrix}\ \{y := y \cdot x;\}\ \begin{pmatrix} i - 1 \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \end{pmatrix}$	12
14	$\begin{pmatrix} i - 1 \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \end{pmatrix}\ \{i\texttt{--};\}\ \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \end{pmatrix}$	ax
15	$\begin{pmatrix} i \geq 0 \wedge \\ y \cdot x \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \\ \wedge\ i > 0 \end{pmatrix}\ \{y := y \cdot x; i\texttt{--};\}\ \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \end{pmatrix}$	13, 14
16	$\begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \\ \wedge\ i > 0 \end{pmatrix}\ \{y := y \cdot x; i\texttt{--};\}\ \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \end{pmatrix}$	8, 15
17	$\begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \end{pmatrix}\ \{\mathsf{C}\}\ \begin{pmatrix} i \geq 0 \wedge \\ y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \wedge i \not> 0 \end{pmatrix}$	16
18	$(i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n))\,\{\mathsf{C}\}\,(y = \mathrm{p}(x,n) \wedge i \not> 0)$	7, 17
19	$(n \geq 0 \wedge i = n \wedge y = 1)\,\{\mathsf{C}\}\,(y = \mathrm{p}(x,n) \wedge i \not> 0)$	6, 18
20	$n \geq 0\,\{i := n; y := 1; \mathsf{C}\}\,(y = \mathrm{p}(x,n) \wedge i \not> 0)$	11, 19
21	$n \geq 0\,\{i := n; y := 1; \mathsf{C}\}\,y = \mathrm{p}(x,n)$	20
22	$n \geq 0\,\{i := n; y := 1; \texttt{while}\ (i > 0)\ \{y := y \cdot x; i\texttt{--};\}\}\,y = \mathrm{p}(x,n)$	5, 21
23	$n \geq 0\,\{i := n; y := 1; \texttt{while}\ (i > 0)\ \{y := y \cdot x; i\texttt{--};\}\}\,y = \mathrm{p}(x,n)$	5, 22
24	$n \geq 0\,\{\texttt{int}\ i; i := n; y := 1; \texttt{while}\ (i > 0)\ \{y := y \cdot x; i\texttt{--};\}\}\,y = \mathrm{p}(x,n)$	4, 23

Commentaires

– la preuve *sous-entend* les axiomes de l'arithmetique
– l'expression i-- est une abréviation pour l'expression $i := i - 1$
– l'invariante de la boucle `while` est mise en évidence en rouge
– le programme termine parce que i décroît *strictement*

Lemme (1)

5.1	$n \geq 0 \wedge i = n \wedge y = 1$	hyp
5.2	$i \geq 0$	5.1
5.3	$\mathrm{p}(x, i) = \mathrm{p}(x, i)$	théor
5.4	$\mathrm{p}(x, i) = \mathrm{p}(x, n)$	5.1, 5.3
5.5	$1 \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n)$	5.4
5.6	$y \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n)$	5.1, 5.5
5.7	$i \geq 0 \wedge y \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n)$	5.2 5.6
6	$(n \geq 0 \wedge i = n \wedge y = 1) \Rightarrow (i \geq 0 \wedge y \cdot \mathrm{p}(x, i) = \mathrm{p}(x, n))$	5.1, 5.7

Lemme (2)

6.1	$i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \wedge i \not> 0$	hyp
6.2	$i = 0$	6.1
6.3	$\mathrm{p}(x,i) = 1$	1, 6.2
6.4	$y \cdot 1 = \mathrm{p}(x,n)$	6.1, 6.3
6.5	$y = \mathrm{p}(x,n)$	6.4
6.6	$y = \mathrm{p}(x,n) \wedge i \not> 0$	6.1, 6.5
7	$(i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \wedge i \not> 0) \Rightarrow (y = \mathrm{p}(x,n) \wedge i \not> 0)$	6.1, 6.6

Lemme (3)

7.1	$i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \wedge i > 0$	hyp
7.2	$i \geq 1$	7.1
7.3	$\mathrm{p}(x,i) = x \cdot \mathrm{p}(x,i-1)$	2, 7.2
7.4	$y \cdot x \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n)$	7.1, 7.3
7.5	$i \geq 0 \wedge y \cdot x \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \wedge i > 0$	7.1, 7.4
8	$(i \geq 0 \wedge y \cdot \mathrm{p}(x,i) = \mathrm{p}(x,n) \wedge i > 0) \Rightarrow$ $(i \geq 0 \wedge y \cdot x \cdot \mathrm{p}(x,i-1) = \mathrm{p}(x,n) \wedge i > 0)$	7.1, 7.5