Étude de cas 6°

Preuve de programme

Recherche dichotomique dans un tableau trié

15 juin 2004

Nous allons prouver que le programme

```
const int max;
int n;
Typename Entry;
const Entry x;
const Entry A[max];
bool present;
{
  int left, right;
  left := 0;
  right := n − 1;
  while (left ≠ right)
  {
    int mid;
    mid := (left + right)/2;
    if (x ≤ A[mid]) then right := mid; else left := mid + 1;
  }
  present := A[right] = x;
}
```

trouve un élément x dans le segment $A[0:n-1]$ — *trié dans l'ordre croissant* — du tableau A si et seulement si x s'y trouve effectivement.

Dans ce but, nous allons

1. déterminer la pré-condition (c'est une conjonction de deux autres conditions)
2. prouver formellement — moyennant la logique de Hoare — que $present \Leftrightarrow x \in A[0:n-1]$ *si le programme termine*, en prenant comme *invariante*

$$A[0:n-1]\uparrow \wedge 0 \leq left \leq right \leq n-1 \leq max-1 \wedge$$
$$x \in A[0:n-1] \Rightarrow (x \geq A[0:left] \;\wedge\; x \leq A[right:n-1])$$

3. prouver informellement que le programme termine.

Preuve formelle

1	$\forall(1 \leq max \in \texttt{int})\forall(A \in \texttt{Entry}^{max})$ $A\uparrow \Leftrightarrow \forall(0 \leq i,j \leq max-1)(i<j \Rightarrow A[i] \leq A[j])$	ax déf
2	$max \in \texttt{int} \wedge n \in \texttt{int} \wedge A \in \texttt{Entry}^{max} \wedge x \in \texttt{Entry} \wedge present \in \texttt{bool}$	hyp
3	$left \in \texttt{int}$	hyp
4	$right \in \texttt{int}$	hyp
5	$I = A[0:n-1]\uparrow \wedge 0 \leq left \leq right \leq n-1 \leq max-1 \wedge$ $x \in A[0:n-1] \Rightarrow (x \geq A[0:left] \wedge x \leq A[right:n-1])$	hyp
6	$(A[0:n-1]\uparrow \wedge 1 \leq n \leq max)$ $\{left := 0;\}$ $(A[0:n-1]\uparrow \wedge 1 \leq n \leq max \wedge left = 0)$	ax
7	$(A[0:n-1]\uparrow \wedge 1 \leq n \leq max \wedge left = 0)$ $\{right := n-1;\}$ $(A[0:n-1]\uparrow \wedge 1 \leq n \leq max \wedge left = 0 \wedge right = n-1)$	ax
8	$(A[0:n-1]\uparrow \wedge 1 \leq n \leq max)$ $\{left := 0; right := n-1;\}$ $(A[0:n-1]\uparrow \wedge 1 \leq n \leq max \wedge left = 0 \wedge right = n-1)$	6, 7
9	$(A[0:n-1]\uparrow \wedge 1 \leq n \leq max \wedge left = 0 \wedge right = n-1) \Rightarrow I$	lem 1
10	$(A[0:n-1]\uparrow \wedge 1 \leq n \leq max)\,\{left := 0; right := n-1;\}\,I$	8, 9
11	$mid \in \texttt{int}$	hyp
12	$(I \wedge left \neq right)$ $\{mid := (left+right)/2;\}$ $(I \wedge left \neq right \wedge mid = (left+right)/2)$	ax
13	$(I \wedge left \neq right \wedge mid = (left+right)/2) \Rightarrow$ $(I \wedge left \leq mid < right)$	lem 2
14	$(I \wedge left \neq right)\,\{mid := (left+right)/2;\}\,(I \wedge left \leq mid < right)$	12, 13
15	$[mid/right](I \wedge left \leq mid \leq right \wedge x \leq A[mid])$ $\{right := mid;\}$ $(I \wedge left \leq mid \leq right \wedge x \leq A[mid] \wedge right = mid)$	ax
16	$(I \wedge left \leq mid \leq right \wedge x \leq A[mid]) \Rightarrow$ $[mid/right](I \wedge left \leq mid \leq right \wedge x \leq A[mid])$	lem 3
17	$(I \wedge left \leq mid \leq right \wedge x \leq A[mid])$ $\{right := mid;\}$ $(I \wedge left \leq mid \leq right \wedge x \leq A[mid] \wedge right = mid)$	15, 16
18	$(I \wedge left \leq mid \leq right \wedge x \leq A[mid])\,\{right := mid;\}\,I$	17
19	$(I \wedge left \leq mid < right \wedge x \leq A[mid])\,\{right := mid;\}\,I$	18

20 $[mid+1/left](I \wedge 0 \leq mid < right \wedge x \nleq A[mid])$
$\{left := mid+1;\}$
$(I \wedge 0 \leq mid < right \wedge x \nleq A[mid] \wedge left = mid+1)$ ax

21 $(I \wedge 0 \leq mid < right \wedge x \nleq A[mid]) \Rightarrow$
$[mid+1/left](I \wedge 0 \leq mid < right \wedge x \nleq A[mid])$ lem 4

22 $(I \wedge 0 \leq mid < right \wedge x \nleq A[mid])$
$\{left := mid+1;\}$
$(I \wedge 0 \leq mid < right \wedge x \nleq A[mid] \wedge left = mid+1)$ 20, 21

23 $(I \wedge 0 \leq mid < right \wedge x \nleq A[mid])\,\{left := mid+1;\}\,I$ 22

24 $(I \wedge left \leq mid < right \wedge x \nleq A[mid])\,\{left := mid+1;\}\,I$ 23

25 $(I \wedge left \leq mid < right)$
$\{\texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;\}$
I 19, 24

26 $(I \wedge left \neq right)$
$\{$
$\quad mid := (left + right)/2;$
$\quad \texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
$\}$
I 14, 25

27 $(I \wedge left \neq right)$
$\{$
$\quad \texttt{int}\ mid;$
$\quad mid := (left + right)/2;$
$\quad \texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
$\}$
I 11, 26

28 I
$\{$
$\quad \texttt{while}\ (left \neq right)$
$\quad \{$
$\qquad \texttt{int}\ mid;$
$\qquad mid := (left + right)/2;$
$\qquad \texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
$\quad \}$
$\}$
$(I \wedge left = right)$ 27

Simon Kramer Logique élémentaire EPFL

29 $(I \wedge left = right)$
$\{present := A[right] = x;\}$
$(I \wedge left = right \wedge present = (A[right] = x))$ ax

30 $(I \wedge left = right \wedge present = (A[right] = x)) \Rightarrow$
$present \Leftrightarrow x \in A[0:n-1]$ lem 5

31 $(I \wedge left = right)$
$\{present := A[right] = x;\}$
$present \Leftrightarrow x \in A[0:n-1]$ 29, 30

32 I
$\{$
$\quad \texttt{while}\ (left \neq right)$
$\quad \{$
$\qquad \texttt{int}\ mid;$
$\qquad mid := (left + right)/2;$
$\qquad \texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
$\quad \}$
$\quad present := A[right] = x;$
$\}$
$present \Leftrightarrow x \in A[0:n-1]$ 28, 31

33 $(A[0:n-1]\uparrow \wedge 1 \leq n \leq max)$
$\{$
$\quad left := 0;$
$\quad right := n-1;$
$\quad \texttt{while}\ (left \neq right)$
$\quad \{$
$\qquad \texttt{int}\ mid;$
$\qquad mid := (left + right)/2;$
$\qquad \texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
$\quad \}$
$\quad present := A[right] = x;$
$\}$
$present \Leftrightarrow x \in A[0:n-1]$ 10, 32

34

$(A[0:n-1]{\uparrow} \wedge 1 \leq n \leq max)$
{
  $left := 0;$
  $right := n-1;$
  $\texttt{while}\ (left \neq right)$
  {
    $\texttt{int}\ mid;$
    $mid := (left + right)/2;$
    $\texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
  }
  $present := A[right] = x;$
}
$present \Leftrightarrow x \in A[0:n-1]$

5, 33

35

$(A[0:n-1]{\uparrow} \wedge 1 \leq n \leq max)$
{
  $\texttt{int}\ right;$
  $left := 0;$
  $right := n-1;$
  $\texttt{while}\ (left \neq right)$
  {
    $\texttt{int}\ mid;$
    $mid := (left + right)/2;$
    $\texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
  }
  $present := A[right] = x;$
}
$present \Leftrightarrow x \in A[0:n-1]$

4, 34

36

$(A[0:n-1]{\uparrow} \wedge 1 \leq n \leq max)$
{
  $\texttt{int}\ left;$
  $\texttt{int}\ right;$
  $left := 0;$
  $right := n-1;$
  $\texttt{while}\ (left \neq right)$
  {
    $\texttt{int}\ mid;$
    $mid := (left + right)/2;$
    $\texttt{if}\ (x \leq A[mid])\ \texttt{then}\ right := mid;\ \texttt{else}\ left := mid+1;$
  }
  $present := A[right] = x;$
}
$present \Leftrightarrow x \in A[0:n-1]$

3, 35

Commentaires

– $\uparrow$ est un symbole relationnel unaire post-fixe prononcé « est trié dans l'ordre croissant »
– la preuve sous-entend les axiomes de l'arithmétique ainsi que les axiomes régissant l'opération de division $/$ retournant la partie entière (sans reste) d'une division
– le programme termine parce que la boucle assure que la différence de $right$ et $left$ décroît *strictement*

Lemme (1)

8.1	$A[0:n-1]\!\uparrow \wedge 1 \leq n \leq max \wedge left = 0 \wedge right = n-1$	hyp
8.2	$0 \leq left$	8.1
8.3	$0 \leq n-1$	8.1
	$= right$	8.1
8.4	$left \leq right$	8.1, 8.3
8.5	$right \leq n-1$	8.1
8.6	$n-1 \leq max-1$	8.1
8.7	$0 \leq left \leq right \leq n-1 \leq max-1$	8.2, 8.4–8.6
8.8	$x \in A[0:n-1]$	hyp
8.9	$\exists(0 \leq i \leq n-1)(x = A[i])$	8.8
8.10	$0 \leq i \leq n-1 \wedge x = A[i]$	hyp
8.11	$i = 0 \vee 0 < i < n-1 \vee i = n-1$	8.10
8.12	$i = 0$	hyp
	⋮	
8.39	$x \geq A[0:left] \wedge x \leq A[right:n-1]$	8.21, 8.38
8.40	$0 < i < n-1$	hyp
	⋮	
8.58	$x \geq A[0:left] \wedge x \leq A[right:n-1]$	8.48, 8.57
8.59	$i = n-1$	hyp
	⋮	
8.86	$x \geq A[0:left] \wedge x \leq A[right:n-1]$	8.76, 8.85
8.87	$x \geq A[0:left] \wedge x \leq A[right:n-1]$	8.11, 8.12, 8.40, 8.59
8.88	$x \geq A[0:left] \wedge x \leq A[right:n-1]$	8.9, 8.87
8.89	$x \in A[0:n-1] \Rightarrow (x \geq A[0:left] \wedge x \leq A[right:n-1])$	8.8, 8.88
8.90	I	8.1, 8.7, 8.89
9	$(A[0:n-1]\!\uparrow \wedge 1 \leq n \leq max \wedge left = 0 \wedge right = n-1) \Rightarrow I$	8.1, 8.90

8.13	$0 \leq k \leq left$	hyp
8.14	$0 \leq k \leq 0$	8.1, 8.13
8.15	$k = 0$	8.14
8.16	$i = k$	8.12, 8.15
8.17	$x = x$	ax
	$= A[i]$	8.10
	$= A[k]$	8.16
8.18	$x \geq A[k]$	8.17
8.19	$0 \leq k \leq left \Rightarrow x \geq A[k]$	8.13, 8.18
8.20	$\forall(0 \leq k \leq left)(x \geq A[k])$	8.19
8.21	$x \geq A[0:left]$	8.20
8.22	$right \leq k \leq n-1$	hyp
8.23	$n-1 \leq k \leq n-1$	8.1, 8.22
8.24	$k = n-1$	8.23
8.25	$1 = n \vee 1 < n$	8.1
8.26	$1 = n$	hyp
8.27	$k = 0$	8.24, 8.26
	$= i$	8.12
8.28	$x = x$	ax
	$= A[i]$	8.10
	$= A[k]$	8.27
8.29	$x \leq A[k]$	8.28
8.30	$1 < n$	hyp
8.31	$0 < n-1$	8.30
	$= k$	8.24
8.32	$i < k$	8.12, 8.31
8.33	$A[i] \leq A[k]$	8.1, 8.32
8.34	$x \leq A[k]$	8.10, 8.33
8.35	$x \leq A[k]$	8.25, 8.26, 8.30
8.36	$right \leq k \leq n-1 \Rightarrow x \leq A[k]$	8.22, 8.35
8.37	$\forall(right \leq k \leq n-1)(x \leq A[k])$	8.36
8.38	$x \leq A[right:n-1]$	8.37

8.41	$0 \leq k \leq \mathit{left}$	hyp
8.42	$0 \leq k \leq 0$	8.1, 8.41
8.43	$k = 0$	8.42
8.44	$k < i$	8.40, 8.43
8.45	$A[k] \leq A[i]$	8.1, 8.44
	$= x$	8.10
8.46	$0 \leq k \leq \mathit{left} \Rightarrow x \geq A[k]$	8.41, 8.45
8.47	$\forall(0 \leq k \leq \mathit{left})(x \geq A[k])$	8.46
8.48	$x \geq A[0 : \mathit{left}]$	8.47
8.49	$\mathit{right} \leq k \leq n-1$	hyp
8.50	$n-1 \leq k \leq n-1$	8.1, 8.49
8.51	$k = n-1$	8.50
8.52	$i < k$	8.40, 8.51
8.53	$A[i] \leq A[k]$	8.1, 8.52
8.54	$x \leq A[k]$	8.10, 8.53
8.55	$\mathit{right} \leq k \leq n-1 \Rightarrow x \leq A[k]$	8.49, 8.54
8.56	$\forall(\mathit{right} \leq k \leq n-1)(x \leq A[k])$	8.55
8.57	$x \leq A[\mathit{right} : n-1]$	8.56

8.60	$0 \leq k \leq \mathit{left}$	hyp
8.61	$0 \leq k \leq 0$	8.1, 8.60
8.62	$k = 0$	8.61
8.63	$1 = n \vee 1 < n$	8.1
8.64	$1 = n$	hyp
8.65	$i = 0$	8.59, 8.64
8.66	$i = k$	8.62, 8.65
8.67	$x = x$	ax
	$= A[i]$	8.10
	$= A[k]$	8.66
8.68	$x \geq A[k]$	8.67
8.69	$1 < n$	hyp
	$= i + 1$	8.59
8.70	$0 < i$	8.69
8.71	$k < i$	8.62, 8.70
8.72	$A[k] \leq A[i]$	8.1, 8.71
	$= x$	8.10
8.73	$x \geq A[k]$	8.63, 8.64, 8.69
8.74	$0 \leq k \leq \mathit{left} \Rightarrow x \geq A[k]$	8.60, 8.73
8.75	$\forall(0 \leq k \leq \mathit{left})(x \geq A[k])$	8.74
8.76	$x \geq A[0 : \mathit{left}]$	8.75
8.77	$\mathit{right} \leq k \leq n-1$	hyp
8.78	$n-1 \leq k \leq n-1$	8.1
8.79	$k = n-1$	8.78
8.80	$i = k$	8.59, 8.79
8.81	$x = x$	ax
	$= A[i]$	8.10
	$= A[k]$	8.80
8.82	$x \leq A[k]$	8.81
8.83	$\mathit{right} \leq k \leq n-1 \Rightarrow x \leq A[k]$	8.77, 8.82
8.84	$\forall(\mathit{right} \leq k \leq n-1)(x \leq A[k])$	8.83
8.85	$x \leq A[\mathit{right} : n-1]$	8.84

Lemme (2)

12.1	$I \wedge left \neq right \wedge mid = (left + right)/2$	hyp
12.2	$left < right$	12.1
12.3	$mid < (right + right)/2$	12.1, 12.2
	$= right$	
12.4	$mid \geq (left + left)/2$	12.1, 12.2
	$= left$	
12.5	$I \wedge left \leq mid < right$	12.1, 12.3, 12.4
13	$(I \wedge left \neq right \wedge mid = (left + right)/2) \Rightarrow (I \wedge left \leq mid < right)$	12.1, 12.3

Simon Kramer Logique élémentaire EPFL

Lemme (3)

15.1	$I \wedge left \leq mid \leq right \wedge x \leq A[mid]$	hyp
15.2	$left \leq mid$	15.1
15.3	$mid \leq n - 1$	15.1
15.4	$0 \leq left \leq mid \leq n - 1 \leq max - 1$	15.1–15.3
15.5	$mid \leq mid$	ax
15.6	$left \leq mid \leq mid$	15.1, 15.5
15.7	$x \in A[0 : n - 1]$	hyp
15.8	$mid \leq k \leq n - 1$	hyp
15.9	$mid = k \vee mid < k < n - 1 \vee k = n - 1$	15.8
15.10	$mid = k$	hyp
15.11	$x \leq A[k]$	15.1, 15.10
15.12	$mid < k < n - 1$	hyp
15.13	$A[mid] \leq A[k]$	15.1, 15.12
15.14	$x \leq A[k]$	15.1, 15.13
15.15	$k = n - 1$	hyp
15.16	$mid \leq n - 1$	15.3
15.17	$mid = n - 1 \vee mid < n - 1$	15.16
15.18	$mid = n - 1$	hyp
15.19	$k = mid$	15.15, 15.18
15.20	$x \leq A[k]$	15.1, 15.19
15.21	$mid < n - 1$	hyp
15.22	$A[mid] \leq A[n - 1]$	15.1, 15.21
	$= A[k]$	15.15
15.23	$x \leq A[k]$	15.1, 15.22
15.24	$x \leq A[k]$	15.(17, 18, 21)
15.25	$x \leq A[k]$	15.(9, 10, 12, 15)
15.26	$mid \leq k \leq n - 1 \Rightarrow x \leq A[k]$	15.8, 15.25
15.27	$\forall(mid \leq k \leq n - 1)(x \leq A[k])$	15.26
15.28	$x \leq A[mid : n - 1]$	15.27
15.29	$x \geq A[0 : left] \wedge x \leq A[mid : n - 1]$	15.1, 15.7, 15.28
15.30	$x \in A[0 : n - 1] \Rightarrow (x \geq A[0 : left] \wedge x \leq A[mid : n - 1])$	15.7, 15.29
15.31	$[mid/right](I \wedge left \leq mid \leq right \wedge x \leq A[mid])$	15.(1, 4, 6, 30)
16	$(I \wedge left \leq mid \leq right \wedge x \leq A[mid]) \Rightarrow [mid/right](I \wedge left \leq mid \leq right \wedge x \leq A[mid])$	15.1, 15.31

Lemme (4)

20.1	$I \wedge 0 \leq mid < right \wedge x \not\leq A[mid]$	hyp
20.2	$mid + 1 \leq right$	20.1
20.3	$0 \leq mid + 1 \leq right \leq n - 1 \leq max - 1$	20.1, 20.2
20.4	$x \in A[0 : n - 1]$	hyp
20.5	$0 \leq i \leq mid + 1$	hyp
20.6	$\exists(0 \leq j \leq n - 1)(x = A[j])$	20.4
20.7	$0 \leq j \leq n - 1 \wedge x = A[j]$	hyp
20.8	$x > A[mid]$	20.1
20.9	$A[j] > A[mid]$	20.8
20.10	$j \not> mid$	hyp
	$\vdots$	
20.19	$\bot$	20.(12, 13, 16)
20.20	$j > mid$	20.10
20.21	$j \geq mid + 1$	20.20
20.22	$i \leq j$	20.5, 20.21
20.23	$i < j \vee i = j$	20.22
20.24	$i < j$	hyp
20.25	$A[i] \leq A[j]$	20.1, 20.24
	$= x$	20.7
20.26	$i = j$	hyp
20.27	$A[j] \geq A[j]$	ax
20.28	$x \geq A[i]$	20.7, 20.26
20.29	$x \geq A[i]$	20.(23, 24, 26)
20.30	$x \geq A[i]$	20.6, 20.29
20.31	$0 \leq i \leq mid + 1 \Rightarrow x \geq A[i]$	20.5, 20.30
20.32	$\forall(0 \leq i \leq mid + 1)(x \geq A[i])$	20.31
20.33	$x \geq A[0 : mid + 1]$	20.32
20.34	$x \geq A[0 : mid + 1] \wedge x \leq A[right : n - 1]$	20.(1, 4, 33)
20.35	$x \in A[0 : n - 1] \Rightarrow$	
	$(x \geq A[0 : mid + 1] \wedge x \leq A[right : n - 1])$	20.4, 20.34
20.36	$[mid + 1/left](I \wedge 0 \leq mid < right \wedge x \not\leq A[mid])$	20.(1, 3, 35)
21	$(I \wedge 0 \leq mid < right \wedge x \not\leq A[mid]) \Rightarrow$	
	$[mid + 1/left](I \wedge 0 \leq mid < right \wedge x \not\leq A[mid])$	20.1, 20.36

Simon Kramer Logique élémentaire EPFL

20.11	$j \leq mid$	20.10
20.12	$j < mid \vee j = mid$	20.11
20.13	$j < mid$	hyp
20.14	$A[j] \leq A[mid]$	20.1, 20.13
20.15	$\bot$	20.9, 20.14
20.16	$j = mid$	hyp
20.17	$A[j] = A[j]$	ax
	$= A[mid]$	20.16
20.18	$\bot$	20.9, 20.17

Lemme (5)

29.1	$I \wedge left = right \wedge present = (A[right] = x)$	hyp
29.2	$present$	hyp
29.3	$A[right] = x$	29.1, 29.2
29.4	$0 \leq right \leq n - 1$	29.1
29.5	$\exists(0 \leq i \leq n - 1)(x = A[i])$	29.3, 29.4
29.6	$x \in A[0 : n - 1]$	29.5
29.7	$x \in A[0 : n - 1]$	hyp
29.8	$x \geq A[0 : left] \wedge x \leq A[right : n - 1]$	29.1, 29.7
29.9	$x \geq A[0 : right] \wedge x \leq A[right : n - 1]$	29.1, 29.8
29.10	$A[right] = x$	29.9
29.11	$present$	29.10, 29.10
29.12	$present \Leftrightarrow x \in A[0 : n - 1]$	29.2, 29.7
30	$(I \wedge left = right \wedge present = (A[right] = x)) \Rightarrow present \Leftrightarrow x \in A[0 : n - 1]$	29.1, 29