① Ambiguities: 1. Which program declares the variable marking the boundary? (calling or called subprogram?)

2. Name of this variable?

3. Should this variable mark the left or right side of the boundary?

4. Name of this subprogram

Clarification: Ask the system designer to specify the interface properly and unambiguously.

Adequacy: Sufficiently detailed that the programmers of the calling and called subprograms can design their parts independently, referring only to the interface specification (V, P, relationship between the structure of initial and final data environments)

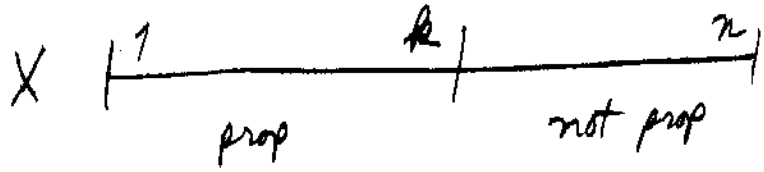
For whom: 1. Person designing the calling subprogram

2. Person designing the called (this) subprogram

3. Persons "maintaining" this subprogram later.

4. Inspectors, reviewers, testers.

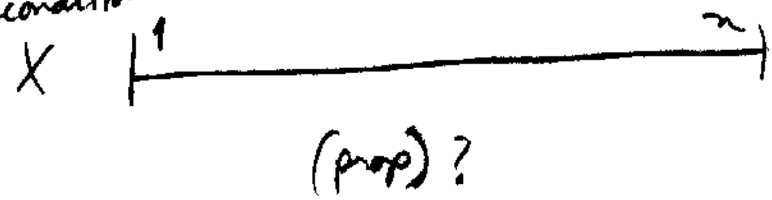
(2) Post condition P :



$$\left[\begin{array}{l} n\in\mathbb{Z} \wedge k\in\mathbb{Z} \wedge 0 \le k \le n \\ \quad \text{and}_{i=1}^{k}\ \text{prop}(X(i)) \quad \text{and}_{i=k+1}^{n}\ \text{not prop}(X(i)) \\ \quad \text{and}\ \left[\&_{i=1}^{n}\ [X(i)]\right]\ \text{Perm}\ \left[\&_{i=1}^{n}\ [X(i)']\right] \end{array}\right]$$

Precondition V :

(3)



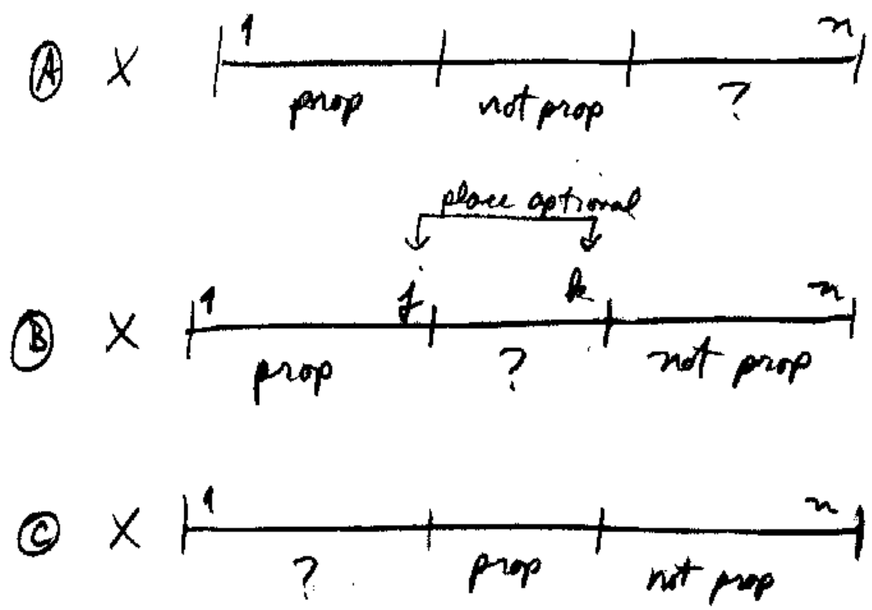
$$\left[\ n\in\mathbb{Z} \wedge 0 \le n \quad \underbrace{\text{and}_{i=1}^{n}\ X(i)=X(i)'}_{\text{from def. of spec. vbl.}}\right]$$

(4) (A) For all data environments d in the domain of Pgm,

$$Pgm.d = [(k, Z, .)] \& d,$$

except for the values of the variables $X(i)$, $i=1, \dots n$ only.

(B) Pgm terminates



Doesn't really matter much.

(B) Once placed, a value of an element of X never needs to be moved again. (Not a strong argument.)

I: $n \in \mathbb{Z} \wedge k \in \mathbb{Z} \wedge j \in \mathbb{Z} \wedge 0 \le j \le k \le n$

$\text{and}_{i=1}^{j}\ \text{prop}(X(i))$ $\text{and}_{i=k+1}^{n}\ \text{not prop}(X(i))$

and $\left[\&_{i=1}^{n}[X(i)]\right]$ Perm $\left[\&_{i=1}^{n}[X(i)']\right]$

(6) (Iteration over array elements required; this suggests a loop.)

Loop $\rightarrow$ W2

So, $\{V\}$ init $\{I\}$

$I \wedge \neg B \Rightarrow P$

$\{I \wedge B\}\ S\ \{I\}$ and progress toward termination

release at end if needed (see answer to question 4).

⑥ ⓐ Diagram for I becomes diagram for V
if $j = 0$ and $k = n$

Both must be declared because of answer to question 4 (k must be declared, value of j, if present initially, may not be changed).

init : declare (j, Z, 0)
declare (k, Z, n)

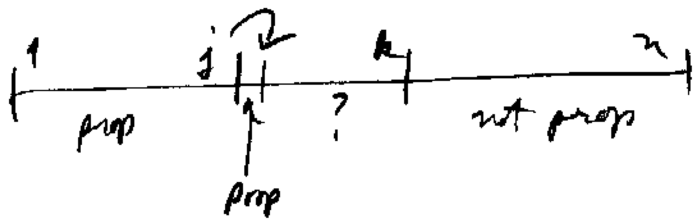
(order does not matter).

ⓑ Diagram for I becomes diagram for P
if $j = k$, So the while condition is $j \neq k$ (or $j < k$).

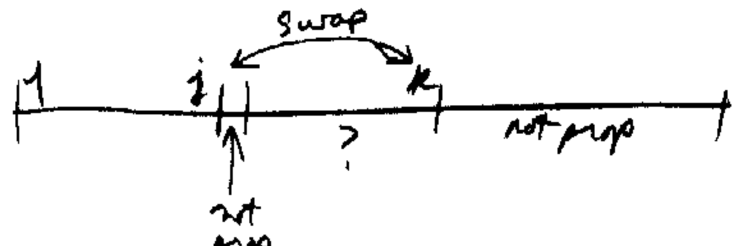
($(j \neq k) = (j < k)$ if I is true).

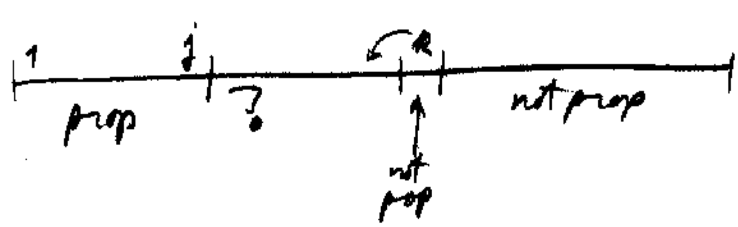
(6) (c) Progress toward termination : increase j by 1 or decrease k by 1. A prerequisite for doing so is that the $X(\ldots)$ has (or does not have) the property prop.

Possibility 1: Examine $X(j+1)$. If prop is true, increase j by one. If prop is not true, swap $X(j+1)$ with $X(k)$ and decrease k by 1:



or






```
if   prop(X(j+1))
then j := j+1
else X(j+1) :=: X(k)
     k := k-1
endif
```

Other possibilities: - Examine X(k) - (symmetrical)
- Examine both X(j+1) and X(k)
(more complicated, does not have a clear advantage).
(If student selects one of these latter possibilities, check for possible violation of loop invariant).

Alternative:

```
if prop (X(k))
then   X(k) :=: X(j+1)
       j := j+1
else   k := k-1
endif
```

Whole program:

```
declare (j, Z, 0); declare (k, Z, n)
while j < k do
  if prop (X(j+1))
  then  j := j+1
  else  X(j+1) :=: X(k)
        k := k-1
  endif
endwhile
release j
```

Alt:

```
if prop(X(k))
then X(k) :=: X(j+1)
     j := j+1
else k := k-1
endif
```

7

$\{V\}\ Pgm\ \{P\}$

$\{V\}$ init; while ... $\{P\}$

W2

$\{V\}$ init $\{I\}$

S2

$V \Rightarrow \left[I^{k}_{n}\right]^{j}_{0}$

a

$\{I \wedge B\} S \{I\}$

IF1

$I \wedge j<k \wedge prop(x(j+1))$
$j := j+1\ \{I\}$*

A2

$I \wedge j<k \wedge prop(x(j+1))$
$\Rightarrow I^{j}_{j+1}$

b

$I \wedge j<k \wedge$ not $prop(x(j+1))$
$x(j+1) := x(k);\ k := k-1$
$\{I\}$*

S2

$I \wedge j<k \wedge$ not $prop(x(j+1))$
$\Rightarrow \left[I^{k}_{k-1}\right]^{x(j+1),\ x(k)}_{x(k),\ x(j+1)}$

c

* strengthening simplifies algebra later

$I \wedge j \geq k \Rightarrow P$

d

(P does not refer to j)

$\{P\}$ release j $\{P\}$

true by SP1

(7) Algebra

(a) $V \Rightarrow [I^k_n]^j_0$?

Proof: $[I^k_n]^j_0$

$=$ $n \in Z \wedge 0 \in Z \wedge 0 \le 0 \le n \le n$

and$_{i=1}^{0}$ ... and$_{i=n+1}^{n}$ ...

and $[\&_{i=1}^{n} [X(i)]]$ Perm $[\&_{i=1}^{n} [X(i)']]$

$=$ $n \in Z \wedge 0 \le n$

and $[\&_{i=1}^{n} [X(i)]]$ Perm $[\&_{i=1}^{n} [X(i)']]$

$\Leftarrow$ $n \in Z \wedge 0 \le n$ and$_{i=1}^{n}$ $X(i) = X(i)'$

$=$ V.

7 (b) $I \wedge j<k \wedge prop(x(j+1)) \Rightarrow I^{j}_{j+1}$?

Proof: I^{j}_{j+1}

$=$

$n \in \mathbb{Z} \wedge k \in \mathbb{Z} \wedge j \in \mathbb{Z} \wedge 0 \le j+1 \le k \le n$

and$_{i=1}^{j+1}$ prop(x(i)) and$_{i=k+1}^{n}$ not prop(x(i))

and ... Perm ...

$\Leftarrow$ [2 steps involved; strengthen lower bound on j; remove term from and series.

$n \in \mathbb{Z} \wedge k \in \mathbb{Z} \wedge j \in \mathbb{Z} \wedge 0 \le j < k \le n$

and prop(x(j+1))

and$_{i=1}^{j}$ prop(x(i)) and$_{i=k+1}^{n}$ not prop(x(i))

and ... Perm ...

$=$

$I \wedge j<k \wedge prop(x(j+1))$ ✓

(7c) $I \wedge j < k \wedge \text{not } prop(x(j+1))$
$$\Rightarrow \left[I^{k}_{k-1} \right]^{x(j+1),\, x(k)}_{x(k),\, x(j+1)} \quad ?$$

$$\left[I^{k}_{k+1} \right]^{x(j+1),\, x(k)}_{x(k),\, x(j+1)}$$

$=$

$$\Big[n \in Z \wedge k \in Z \wedge j \in Z \wedge 0 \le j \le k-1 \le n$$
$$\text{and}_{i=1}^{j}\ prop(x(i)) \text{ and}_{i=k}^{n} \text{ not } prop(x(i))$$
$$\text{and } \dots \text{ Perm } \dots \Big]^{x(j+1),\, x(k)}_{x(k),\, x(j+1)}$$

$\Leftarrow$

$$\Big[n \in Z \wedge k \in Z \wedge j \in Z \wedge 0 \le j < k \le n$$
$$\text{and}_{i=1}^{j}\ prop(x(i)) \text{ and}_{i=k}^{n} \text{ not } prop(x(i))$$
$$\text{and } \dots \text{ Perm } \dots \Big]^{x(j+1),\, x(k)}_{x(k),\, x(j+1)}$$

$=$

$$\Big[n \in Z \wedge k \in Z \wedge j \in Z \wedge 0 \le j < k \le n$$
$$\text{and not } prop(x(k))$$
$$\text{and}_{i=1}^{j}\ prop(x(i)) \text{ and}_{i=k+1}^{n} \text{ not } prop(x(i))$$
$$\text{and } \dots \text{ Perm } \dots \Big]^{x(j+1),\, x(k)}_{x(k),\, x(j+1)}$$

$=$ [$x(j+1), x(k)$ are swapped in the left Perm term, but Perm remains true]

$n \in Z \wedge k \in Z \wedge j \in Z \wedge 0 \le j < k \le n$ and not $prop(x(j+1))$
and$_{i=1}^{j}$ $prop(x(i))$ and$_{i=k+1}^{n}$ not $prop(x(i))$
and ... Perm ...

$=$

$I \wedge j < k$ and not $prop(x(j+1))$ ✓

(7d) $I \wedge j \geq k \Rightarrow P$?

Proof: $I \wedge j \geq k$

$=$

$n \in \mathbb{Z} \wedge k \in \mathbb{Z} \wedge j \in \mathbb{Z} \wedge 0 \leq j = k \leq n$

and$_{i=1}^{j}$ $prop(x(i))$ and$_{i=k+1}^{n}$ not $prop(x(i))$

and ... Perm ...

$\Rightarrow$

$n \in \mathbb{Z} \wedge k \in \mathbb{Z} \wedge 0 \leq k \leq n$

and$_{i=1}^{k}$ $prop(x(i))$ and$_{i=k+1}^{n}$ not $prop(x(i))$

and ... Perm ...

$=$

P ✓