Software Testing & Verification Proof Assignment

Jarno le Conte 3725154
Bas Meesters 3700569

June 22, 2013

Task 1

Simple variant:

$\{*N \geq 0 \wedge sorted\ a\ N*\}$

found := false;
i := 0;
while i < N do { found := found ∨ (a[i]=x) ; i:= i+1}

{*return=(i=N, found = $(\exists i : 0 \leq i \leq N : a[i] = x)$)*}

Variant with breaks:
{*$N \geq 0 \wedge sorted\ a\ N$*}

found := false;
i := 0;
while $i < N \wedge \neg found \wedge a[i] \leq x$ *do* {
    found := found ∨$(a[i] = x)$;
    i := i + 1
}

{*return=$(0 \leq i < N$, found = $(\exists i : 0 \leq i \leq N : a[i] = x)$)*}

Task 2

Invariant (I):
$\{*0 \leq i \leq N \wedge (found = (\exists k : 0 \leq k \leq i : a[k] = x)) \wedge sorted\ a\ N*\}$

Statement S is a sequence S1;S2
S1: found := found ∨ (a[i] = x);
S2: i := i + 1;

Guard g:
{ * i < N ∧¬ found ∧ a[i] ≤ x * }

PROOF PEC
[**A1:**] found $= (\exists k : 0 \leq k < i : a[k])$
[**A2:**] $0 \leq i \leq N$
[**A3:**] $i \geq N$
[**G:**] $(i = N) \wedge (found = (\exists k : 0 \leq k < N : a[k] = x)$
BEGIN

1. { combine A2 and A3 }
   $i = N$
2. { from 1 replace i with N in A1 }
   $(found = (\exists k : 0 \leq k < N : a[k]))$
3. { combine 1 and 2 }
   $(i = N) \wedge (found = (\exists k : 0 \leq k < N : a[k]))$

END

PROOF PIC
PIC: $\{*I \wedge g*\}\ S\ \{*I*\}$
[**A1:**] found $= (\exists k : 0 \leq k < i : a[k] = x)$
[**A2:**] $0 \leq i < N$
[**G1:**] wp S I
BEGIN

1. { see calculate wp }
   wp S I $= 0 \leq i + 1 \leq N \wedge ((found \vee a[i] = x) = (\exists k : 0 \leq k < i + 1 : a[k] = x))$

   PROOF calculate wp
   BEGIN

   wp(found := found $\vee$ a[i] $= x$; i := i $+ 1$)$(0 \leq i \leq N \wedge (found = (\exists k : 0 \leq k \leq i : a[k] = x)))$

   1. { wp of statements sequence }
      wp(found := found $\vee$ a[i] $= x$)(wp(i := i $+ 1$)$(0 \leq i \leq N \wedge (found = (\exists k : 0 \leq k < i : a[k] = x)))$
   2. { wp of assignment }
      wp(found := found $\vee$ a[i] $= x$)$(0 \leq i + 1 \leq N \wedge (found = (\exists k : 0 \leq k < i : a[k] = x)))$
   3. { wp of assignment }
      $0 \leq i + 1 \leq N \wedge ((found \vee a[i] = x) = (\exists k : 0 \leq k < i : a[k] = x))$

   END

2 { see subproof equality }
$\exists k : 0 \leq k < i : a[k] = x) \vee (a[i] = x) = (\exists k : 0 \leq k \leq i + 1 : a[k] = x)$

PROOF equality

[some i]

[some k]
[**A1:**] $\exists k : 0 \le k < i : a[k] = x) \vee (a[i] = x)$
[**G:**] $\exists k : 0 \le k < i : a[k] = x) \vee (a[i] = x) = (\exists k : 0 \le k < i + 1 : a[k] = x)$
BEGIN

$\exists k : 0 \le k < i : a[k] = x) \vee (a[i] = x)$

1. { introduce $\exists$ -quantor }
   $\exists k : 0 \le k \le i : a[k] = x) = \exists k : k = 1 : a[i] = x)$
2. { combine domains }
   $\exists k : 0 \le k < i + 1 : a[k] = x)$
3. { we have proven equality } $\exists k : 0 \le k < i : a[k] = x) \vee (a[i] = x) = (\exists k : 0 \le k < i + 1 : a[k] = x)$

END

3. { reversed substitution of A1 in 2 }
   $((found \vee a[i] = x) = (\exists k : 0 \le k \le i + 1 : a[k] = x))$
4. { rewrite A2 }
   $0 \le i + 1 \le N$
5. { combine 3 and 4 }
   $0 \le i + 1 \le N \wedge ((found \vee a[i] = x) = (\exists k : 0 \le k \le i + 1 : a[k] = x)$
6. { we have proved wp by equality on 1 and 5 }
   $wp\, S\, I = 0 \le i + 1 \le N \wedge ((found \vee a[i] = x) = (\exists k : 0 \le k \le i + 1 : a[k] = x))$

END

PROOF PTC1
Termination metric is N - i
[**A1:**] $i \le N$
[**G:**] $N - i \ge 0$
BEGIN

1. { follows from A1 }
   $N - i \ge 0$

END

PROOF PTC2 [**A1:**] $found = (\exists i : 0 \le i < N : a[i] = x)$
[**A2:**] $i \le N$
[**D1:**] $Q = wp(C := m)\, body\, (N - i < C)\, i := 0$
[**G:**] Q BEGIN

1. { calculating wp }
   $N - i < C$
2. { i := i + 1; C := N - i }
   $N - (i + i) < N - i$
3. { rewrite }
   $N - i - 1 < N - i$

4. { follows from 1,2 and 3 }
   Q

END

PROOF Init
[**A1:**] N ≥ 0
[**A2:**] sorted a N
[**G:**] wp = (found := false; i := 0) I
BEGIN

1. { calculate wp }
   found = (∃i : 0 ≤ i < N : a[i] = x)
2. { follows from intialisation }
   found := false; i := 0
3. { follows from 1 and 2 }
   wp

END

Task 3

Invariant (I):
$\{*0 \leq i \leq N \wedge (found = (\exists k : 0 \leq k \leq i : a[k] = x)) \wedge sorted\ a\ N*\}$

Statement S is a sequence S1;S2
S1: found := found ∨ (a[i] = x);
S2: i := i + 1;

Guard g:
{ * i < N ∧¬ found ∧ a[i] ≤ x * }

PROOF PIC
PIC: $\{*I \wedge g*\}\ S\ \{*I*\}$
[**A1:**] found = (∃k : 0 ≤ k < i : a[k] = x)
[**A2:**] 0 ≤ i < N
[**G1:**] wp S I
BEGIN

1. { see calculate wp }
   wp S I = 0 ≤ i + 1 ≤ N ∧ ((found ∨ a[i] = x) = (∃k : 0 ≤ k < i + 1 : a[k] = x))

   PROOF calculate wp
   BEGIN

   wp(found := found ∨ a[i] = x; i := i + 1)(0 ≤ i ≤ N ∧ (found = (∃k : 0 ≤ k ≤ i : a[k] = x)))

1. { wp of statements sequence }
   $\mathtt{wp}(\mathtt{found} := \mathtt{found} \vee \mathtt{a}[\mathtt{i}] = \mathtt{x})(\mathtt{wp}(\mathtt{i} := \mathtt{i}+1)(0 \leq \mathtt{i} \leq \mathtt{N} \wedge (\mathtt{found} = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}))))$
2. { wp of assignment }
   $\mathtt{wp}(\mathtt{found} := \mathtt{found} \vee \mathtt{a}[\mathtt{i}] = \mathtt{x})(0 \leq \mathtt{i}+1 \leq \mathtt{N} \wedge (\mathtt{found} = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x})))$
3. { wp of assignment }
   $0 \leq \mathtt{i}+1 \leq \mathtt{N} \wedge ((\mathtt{found} \vee \mathtt{a}[\mathtt{i}] = \mathtt{x}) = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$

END _____

2 { see subproof equality }
$\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}) \vee (\mathtt{a}[\mathtt{i}] = \mathtt{x}) = (\exists \mathtt{k} : 0 \leq \mathtt{k} \leq \mathtt{i}+1 : \mathtt{a}[\mathtt{k}] = \mathtt{x})$

PROOF equality

[some i]

[some k]
[**A1:**] $\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}) \vee (\mathtt{a}[\mathtt{i}] = \mathtt{x})$
[**G:**] $\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}) \vee (\mathtt{a}[\mathtt{i}] = \mathtt{x}) = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i}+1 : \mathtt{a}[\mathtt{k}] = \mathtt{x})$
BEGIN _____

$\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}) \vee (\mathtt{a}[\mathtt{i}] = \mathtt{x})$

1. { introduce $\exists$ -quantor }
   $\exists \mathtt{k} : 0 \leq \mathtt{k} \leq \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}) = \exists \mathtt{k} : \mathtt{k} = 1 : \mathtt{a}[\mathtt{i}] = \mathtt{x})$
2. { combine domains }
   $\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i}+1 : \mathtt{a}[\mathtt{k}] = \mathtt{x})$
3. { we have proven equality } $\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}) \vee (\mathtt{a}[\mathtt{i}] = \mathtt{x}) = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i}+1 : \mathtt{a}[\mathtt{k}] = \mathtt{x})$

END _____

3. { reversed substitution of A1 in 2 }
   $((\mathtt{found} \vee \mathtt{a}[\mathtt{i}] = \mathtt{x}) = (\exists \mathtt{k} : 0 \leq \mathtt{k} \leq \mathtt{i}+1 : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$
4. { rewrite A2 }
   $0 \leq \mathtt{i}+1 \leq \mathtt{N}$
5. { combine 3 and 4 }
   $0 \leq \mathtt{i}+1 \leq \mathtt{N} \wedge ((\mathtt{found} \vee \mathtt{a}[\mathtt{i}] = \mathtt{x}) = (\exists \mathtt{k} : 0 \leq \mathtt{k} \leq \mathtt{i}+1 : \mathtt{a}[\mathtt{k}] = \mathtt{x})$
6. { we have proved wp by equality on 1 and 5 }
   $\mathtt{wp}\,\mathtt{S}\,\mathtt{I} = 0 \leq \mathtt{i}+1 \leq \mathtt{N} \wedge ((\mathtt{found} \vee \mathtt{a}[\mathtt{i}] = \mathtt{x}) = (\exists \mathtt{k} : 0 \leq \mathtt{k} \leq \mathtt{i}+1 : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$

END _____

PROOF PEC
[**A1:**] $(\mathtt{found} = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$
[**A2:**] $0 \leq \mathtt{i} \leq \mathtt{N}$
[**A3:**] $\mathtt{i} \geq \mathtt{N} \vee \mathtt{a}[\mathtt{i}] > \mathtt{x}$
[**A4:**] $\forall \mathtt{i} : 0 \leq \mathtt{i} < \mathtt{N} : (\forall \mathtt{j} : \mathtt{i} \leq \mathtt{j} < \mathtt{N} : \mathtt{a}[\mathtt{i}] \leq \mathtt{a}[\mathtt{j}]))$
[**G:**] $0 \leq \mathtt{i} \leq \mathtt{N} \wedge (\mathtt{found} = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{N} : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$
BEGIN _____

1. { see subproof breakWithCounter }
   $\texttt{i} \geq \texttt{N} \Rightarrow 0 \leq \texttt{i} \leq \texttt{N} \wedge (\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}))$
   PROOF breakWithCounter
   [**A1:**] $\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x})$
   [**A2:**] $\texttt{i} \geq \texttt{N}$
   [**A3:**] $0 \leq \texttt{i} \leq \texttt{N}$
   [**G:**] $0 \leq \texttt{i} \leq \texttt{N} \wedge (\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}))$
   BEGIN

   1. { combine A2 and A3 }
      $\texttt{i} = \texttt{N}$
   2. { replace in A1 with N }
      $\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x})$
   3. { combine A3 and 2 }
      $0 \leq \texttt{i} \leq \texttt{N} \wedge (\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}))$

   END

2. { see subproof breakWithFound }
   $\texttt{found} \Rightarrow 0 \leq \texttt{i} \leq \texttt{N} \wedge (\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}))$
   PROOF breakWithFound

   [**A1:**] $\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x})$
   [**A2:**] found
   [**A3:**] $0 \leq \texttt{i} \leq \texttt{N}$
   [**G:**] $0 \leq \texttt{i} \leq \texttt{N} \wedge (\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}))$
   BEGIN

   1. { substitute found in A1 with A2 }
      $(\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{i} : \texttt{a}[\texttt{k}] = \texttt{x})$
   2. { domain expanding }
      $(\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{i} \vee \texttt{i} \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x})$
   3. { domain combine }
      $(\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x})$
   4. { equality of 3 and A2 }
      $\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}$
   5. { combine with A3 }
      $0 \leq \texttt{i} \leq \texttt{N} \wedge (\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}))$

   END

3. { see subproof breakWithValue }
   $\texttt{a}[\texttt{i}] > \texttt{x} \Rightarrow 0 \leq \texttt{i} \leq \texttt{N} \wedge (\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x}))$

   PROOF breakWithValue
   [**A1:**] $\texttt{found} = (\exists \texttt{k} : 0 \leq \texttt{k} < \texttt{N} : \texttt{a}[\texttt{k}] = \texttt{x})$
   [**A2:**] $\texttt{a}[\texttt{i}] > \texttt{x}$
   [**A3:**] $0 \leq \texttt{i} \leq \texttt{N}$
   [**A4:**] $(\forall \texttt{i} : 0 \leq \texttt{i} < \texttt{N} : (\forall \texttt{j} : \texttt{i} \leq \texttt{j} < \texttt{N} : \texttt{a}[\texttt{i}] \leq \texttt{a}[\texttt{j}]))$

[**G:**] $0 \leq \mathtt{i} \leq \mathtt{N} \wedge (\mathtt{found} = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{N} : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$

BEGIN

1. { kwantor elimination in A4 }
   $0 \leq \mathtt{i} < \mathtt{N} \Rightarrow (\forall \mathtt{j} : \mathtt{i} \leq \mathtt{j} < \mathtt{N} : \mathtt{a}[\mathtt{i}] \leq \mathtt{a}[\mathtt{j}])$
2. { follows from A3 and 1 }
   $(\forall \mathtt{j} : \mathtt{i} \leq \mathtt{j} < \mathtt{N} : \mathtt{a}[\mathtt{i}] \leq \mathtt{a}[\mathtt{j}])$
3. { follows from 2 and A2 }
   $\neg(\exists \mathtt{j} : \mathtt{i} \leq \mathtt{j} < \mathtt{N} : \mathtt{a}[\mathtt{j}] = \mathtt{x})$
4. { flip domain of 3 }
   $(\exists \mathtt{j} : \mathtt{j} < \mathtt{i} \vee \mathtt{j} \geq \mathtt{N} : \mathtt{a}[\mathtt{j}] = \mathtt{x})$
5. { split kwantor from 4 }
   $(\exists \mathtt{j} : \mathtt{j} < \mathtt{i} \vee : \mathtt{a}[\mathtt{j}] = \mathtt{x}) \vee (\exists \mathtt{j} : \mathtt{j} \geq \mathtt{N} : \mathtt{a}[\mathtt{j}] = \mathtt{x})$
6. { remove second part from 5 }
   $(\exists \mathtt{j} : \mathtt{j} < \mathtt{i} : \mathtt{a}[\mathtt{j}] = \mathtt{x})$
7. { follows from equality of 6 and A1 }
   $(\mathtt{found} = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$
8. { combine with 7 and A3 }
   $0 \leq \mathtt{i} \leq \mathtt{N} \wedge (\mathtt{found} = (\exists \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{N} : \mathtt{a}[\mathtt{k}] = \mathtt{x}))$

END

4. { A3 with 1,2 and 3 will prove G }

END