

Software Testing & Verification Proof Assignment

Jarno le Conte 3725154
Bas Meesters 3700569

June 22, 2013

Task 1

Simple variant:

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

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

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

Variant with breaks:

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

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

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

Task 2

Invariant (I):

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

Statement S is a sequence S1;S2

S1: found := found \vee (a[i] = x);

S2: i := i + 1;

Guard g:

$\{ * i < N \wedge \neg \text{found} \wedge a[i] \leq x * \}$

PROOF PEC

[A1:] $\text{found} = (\exists k : 0 \leq k < i : a[k])$

[A2:] $0 \leq i \leq N$

[A3:] $i \geq N$

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

BEGIN

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

END

PROOF PIC

PIC: $\{ *I \wedge g* \} S \{ *I* \}$

[A1:] $\text{found} = (\exists k : 0 \leq k < i : a[k] = x)$

[A2:] $0 \leq i < N$

[G1:] $\text{wp } S \text{ I}$

BEGIN

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

PROOF calculate wp

BEGIN

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

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

END

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

PROOF equality

[some i]

some k

[A1:] $\exists k : 0 \leq k < i : a[k] = x \vee (a[i] = x)$

[G:] $\exists k : 0 \leq k < i : a[k] = x \vee (a[i] = x) = (\exists k : 0 \leq k < i + 1 : a[k] = x)$

BEGIN

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

1. { introduce \exists -quantor }

$\exists k : 0 \leq k \leq i : a[k] = x = \exists k : k = i : a[i] = x$

2. { combine domains }

$\exists k : 0 \leq k < i + 1 : a[k] = x$

3. { we have proven equality } $\exists k : 0 \leq k < i : a[k] = x \vee (a[i] = x) =$
 $(\exists k : 0 \leq k < i + 1 : a[k] = x)$

END

3. { reversed substitution of A1 in 2 }

$((\text{found} \vee a[i] = x) = (\exists k : 0 \leq k \leq i + 1 : a[k] = x))$

4. { rewrite A2 }

$0 \leq i + 1 \leq N$

5. { combine 3 and 4 }

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

6. { we have proved wp by equality on 1 and 5 }

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

END

PROOF PTC1

Termination metric is $N - i$

[A1:] $i \leq N$

[G:] $N - i \geq 0$

BEGIN

1. { follows from A1 }

$N - i \geq 0$

END

PROOF PTC2 [A1:] $\text{found} = (\exists i : 0 \leq i \leq N : a[i] = x)$

[A2:] $i \leq N$

[D1:] $Q = \text{wp}(C := m) \text{ body } (N - i < C) i := 0$

[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:] $N \geq 0$
 [A2:] sorted a N
 [G:] wp = (found := false; i := 0) I
 BEGIN

1. { calculate wp }
 found = ($\exists i : 0 \leq i < N : a[i] = x$)

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 \vee ($a[i] = x$);
 S2: i := i + 1;

Guard g:
 $\{ * i < N \wedge \neg found \wedge a[i] \leq x * \}$

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

END

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

PROOF equality

[some i]

[some k]

[A1:] $\exists k : 0 \leq k < i : \text{a}[k] = x \vee (\text{a}[i] = x)$

[G:] $\exists k : 0 \leq k < i : \text{a}[k] = x \vee (\text{a}[i] = x) = (\exists k : 0 \leq k < i + 1 : \text{a}[k] = x)$

BEGIN

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

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

END

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

END

PROOF PEC

[A1:] $(\text{found} = (\exists k : 0 \leq k < i : \text{a}[k] = x))$

[A2:] $0 \leq i \leq N$

[A3:] $i \geq N \vee \text{a}[i] > x$

[A4:] $\forall i : 0 \leq i < N : (\forall j : i \leq j < N : \text{a}[i] \leq \text{a}[j])$

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

BEGIN

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

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

END _____

2. { see subproof breakWithFound }
 $\text{found} \Rightarrow 0 \leq i \leq N \wedge (\text{found} = (\exists k : 0 \leq k < N : a[k] = x))$
PROOF breakWithFound
[A1:] $\text{found} = (\exists k : 0 \leq k < N : a[k] = x)$
[A2:] found
[A3:] $0 \leq i \leq N$
[G:] $0 \leq i \leq N \wedge (\text{found} = (\exists k : 0 \leq k < N : a[k] = x))$
BEGIN _____

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

END _____

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

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

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

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

END

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

END



Ik vind het wel belangrijk om die laatste regel er nog aan toe te voegen die ik in mijn document had staan.