Solution For Assignment 3

Bogdan Dumitriu

October 11, 2004

The proof plan:

$\mathtt{ALL(READ\ b:\ bool[],\ READ\ n:\ int,\ OUT\ r:\ bool)}$

$\mathtt{i,\ j:\ int;}$

$\{*\ \mathtt{n} \geq 0,\ \mathtt{see\ PROOF\ Init}\ *\}$

```
{
   i := 0; j := n; r := T;

   {* I, see PROOFs PTC1, PTC2, PEC, PIC. Termination metric : j − i *}

   while i < j ∧ r do
   {
      j := j − 1;
      r := b[i] ∧ b[j];
      i := i + 1
   }
}
```

$\{*\ \mathtt{r} = (\forall \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{n} : \mathtt{b[k]})\ *\}$

ASSUMING

$\mathtt{I} = (\mathtt{r} = (\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}) \vee (\mathtt{j} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b[k]})) \wedge (0 \leq \mathtt{i} \leq \mathtt{n}) \wedge (0 \leq \mathtt{j} \leq \mathtt{n})$

The proof:

PROOF Init

[A1:] $\mathtt{n} \geq 0$
[D1:] $\mathtt{Q} = \mathtt{wp}\ (\mathtt{i} := 0;\ \mathtt{j} := \mathtt{n};\ \mathtt{r} := \mathtt{T})\ \mathtt{I}$
[G1:] $\mathtt{Q}$

BEGIN ____

1 {Rewrite D1 with definition of I and definition of wp}

$\mathtt{Q} = (\mathtt{T} = (\forall \mathtt{k} : (0 \leq \mathtt{k} < 0) \vee (\mathtt{n} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b[k]})) \wedge (0 \leq 0 \leq \mathtt{n}) \wedge (0 \leq 0 \leq \mathtt{n})$

2 {Trivial, from 1, using A1 and 0 ≤ 0}

$\mathtt{Q} = (\mathtt{T} = (\forall \mathtt{k} : (0 \leq \mathtt{k} < 0) \vee (\mathtt{n} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b[k]})) \wedge \mathtt{T} \wedge \mathtt{T}$

3 {Basic equalities of boolean connectors on 2}

$\mathtt{Q} = (\mathtt{T} = (\forall \mathtt{k} : (0 \leq \mathtt{k} < 0) \vee (\mathtt{n} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}]))$

4 {Empty domain conversion on 3}

$\mathtt{Q} = (\mathtt{T} = (\forall \mathtt{k} : \mathtt{F} \vee \mathtt{F} : \mathtt{b}[\mathtt{k}]))$

5 {Basic equalities of boolean connectors on 4}

$\mathtt{Q} = (\mathtt{T} = (\forall \mathtt{k} : \mathtt{F} : \mathtt{b}[\mathtt{k}]))$

6 {Quantification over empty domain on 5}

$\mathtt{Q} = (\mathtt{T} = \mathtt{T})$

7 {Trivial, from 6}

$\mathtt{Q} = \mathtt{T}$

8 {True consequence on 7}

Q

END

PROOF PTC1

[A1:] I
[A2:] $\mathtt{i} < \mathtt{j} \wedge \mathtt{r}$
[D1:] $\mathtt{Q} = \mathtt{wp}\ (\mathtt{C} := \mathtt{j} - \mathtt{i};\ \mathtt{j} := \mathtt{j} - 1;\ \mathtt{r} := \mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j}];\ \mathtt{i} := \mathtt{i} + 1)\ (\mathtt{j} - \mathtt{i} < \mathtt{C})$
[G1:] Q

BEGIN

---

1 {Rewrite D1 with definition of wp}

$\mathtt{Q} = \mathtt{j} - 1 - \mathtt{i} - 1 < \mathtt{j} - \mathtt{i}$

2 {Trivial, from 1}

$\mathtt{Q} = -2 < 0$

3 {Trivial, from 2}

$\mathtt{Q} = \mathtt{T}$

4 {True consequence on 3}

Q

END

PROOF PTC2

[A1:] I
[A2:] $\mathtt{i} < \mathtt{j} \wedge \mathtt{r}$
[G1:] $\mathtt{j} - \mathtt{i} > 0$

BEGIN

---

1 {$\wedge$-Elimination on A2}

$\mathtt{i} < \mathtt{j}$

2 {Trivial, from 1}

$j - i > 0$

END

PROOF PEC

[A1:] I
[A2:] $j \leq i \vee \neg r$
[G1:] $r = (\forall k : 0 \leq k < n : b[k])$

BEGIN

1 {Rewrite A1 with definition of I}

$(r = (\forall k : (0 \leq k < i) \vee (j \leq k < n) : b[k])) \wedge (0 \leq i \leq n) \wedge (0 \leq j \leq n)$

2 {$\wedge$-Elimination on 1}

$r = (\forall k : (0 \leq k < i) \vee (j \leq k < n) : b[k])$

3 {$\wedge$-Elimination on 1}

$0 \leq i \leq n$

4 {$\wedge$-Elimination on 1}

$0 \leq j \leq n$

5 {See subproof sp1}

$j \leq i \Rightarrow (r = (\forall k : 0 \leq k < n : b[k]))$

PROOF sp1

[A1:] $j \leq i$

[G1:] $r = (\forall k : 0 \leq k < n : b[k])$

BEGIN

1 {Domain merging on PEC.2, using $0 \leq j$ (from PEC.4) and A1}
$r = (\forall k : (0 \leq k < j) \vee (j \leq k < i) \vee (j \leq k < n) : b[k])$

2 {From 1, using the fact that $i \leq n$ (from PEC.3) implies that $[j, i)$ is included in $[j, n)$}
$r = (\forall k : (0 \leq k < j) \vee (j \leq k < n) : b[k])$

3 {Domain merging on 2, using PEC.4}
$r = (\forall k : 0 \leq k < n : b[k])$

END

6 {See subproof sp2}

$\neg r \Rightarrow (r = (\forall k : 0 \leq k < n : b[k]))$

PROOF sp2

[A1:] $\neg r$

[G1:] $r = (\forall k : 0 \leq k < n : b[k])$

BEGIN

1 {Rewrite A1 with PEC.2}
$\neg(\forall k : (0 \leq k < i) \vee (j \leq k < n) : b[k])$

2 {Negate $\forall$ on 1}
$(\exists k : (0 \leq k < i) \vee (j \leq k < n) : \neg b[k])$

3 {$\exists$-Elimination on 2}
[SOME k]
$((0 \leq k < i) \vee (j \leq k < n)) \wedge \neg b[k]$

4 {$\wedge$-Elimination on 3}
$(0 \leq k < i) \vee (j \leq k < n)$

5 {$\wedge$-Elimination on 3}
$\neg b[k]$

6 {Trivial, from PEC.3}
$0 \leq k < i \Rightarrow 0 \leq k < n$

7 {Trivial, from PEC.4}
$j \leq k < n \Rightarrow 0 \leq k < n$

8 {Case split on 4, 6 and 7}
$0 \leq k < n$

9 {$\exists$-Introduction on 8 and 5}
$(\exists k : 0 \leq k < n : \neg b[k])$

10 {Negate $\forall$ on 9}
$\neg(\forall k : 0 \leq k < n : b[k])$

11 {False consequence (see proof at the end of the document) on 10}
$(\forall k : 0 \leq k < n : b[k]) = F$

12 {False consequence (see proof at the end of the document) on A1}
$r = F$

13 {Rewrite 12 with 11}
$r = (\forall k : 0 \leq k < n : b[k])$

END

7 Case split on A2, 5 and 6
$r = (\forall k : 0 \leq k < n : b[k])$

END

PROOF PIC

[A1:] I
[A2:] $i < j \wedge r$
[D1:] $Q = wp\ (j := j - 1;\ r := b[i] \wedge b[j];\ i := i + 1)\ I$
[G1:] Q

BEGIN

1 {Rewrite A1 with definition of I}
$(r = (\forall k : (0 \leq k < i) \vee (j \leq k < n) : b[k])) \wedge (0 \leq i \leq n) \wedge (0 \leq j \leq n)$

2 {Rewrite D1 with definition of I and definition of wp}

$\mathtt{Q} = (\mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j}-1] = (\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}+1) \vee (\mathtt{j}-1 \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}]))$
$\wedge\ (0 \leq \mathtt{i}+1 \leq \mathtt{n}) \wedge (0 \leq \mathtt{j}-1 \leq \mathtt{n})$

3 {∧-Elimination on 1}

$\mathtt{r} = (\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}) \vee (\mathtt{j} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}])$

4 {∧-Elimination on 1}

$0 \leq \mathtt{i} \leq \mathtt{n}$

5 {∧-Elimination on 1}

$0 \leq \mathtt{j} \leq \mathtt{n}$

6 {∧-Elimination on A2}

$\mathtt{i} < \mathtt{j}$

7 {∧-Elimination on A2}

$\mathtt{r}$

8 {Trivial, from 6 and j ≤ n (from 5)}

$\mathtt{i} < \mathtt{n}$

9 {Trivial, from 8}

$\mathtt{i}+1 \leq \mathtt{n}$

10 {Trivial, from 0 ≤ i (from 4)}

$0 \leq \mathtt{i}+1$

11 {Conjunction on 9 and 10}

$0 \leq \mathtt{i}+1 \leq \mathtt{n}$

12 {Trivial, from 6 and 0 ≤ i (from 4)}

$0 < \mathtt{j}$

13 {Trivial, from 12}

$0 \leq \mathtt{j}-1$

14 {Trivial, from j ≤ n (from 5)}

$\mathtt{j}-1 \leq \mathtt{n}$

15 {Conjunction on 13 and 14}

$0 \leq \mathtt{j}-1 \leq \mathtt{n}$

16 {See subproof eq}

$\mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j}-1] = (\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}+1) \vee (\mathtt{j}-1 \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}])$

EQUATIONAL PROOF eqq

$(\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}+1) \vee (\mathtt{j}-1 \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}])$

= {By domain merging, justified by 0 ≤ i (from PIC.4)}

$(\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}) \vee (\mathtt{k} = \mathtt{i}) \vee (\mathtt{j}-1 \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}])$

= {By domain merging, justified by j-1 ≤ j and j ≤ n (from PIC.5)}

$(\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}) \vee (\mathtt{k} = \mathtt{i}) \vee (\mathtt{j}-1 \leq \mathtt{k} < \mathtt{j}) \vee (\mathtt{j} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}])$

$= \{\texttt{Trivial:} \quad \mathtt{j} - 1 \leq \mathtt{k} < \mathtt{j} = (\mathtt{k} = \mathtt{j} - 1)\}$

$(\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}) \vee (\mathtt{k} = \mathtt{i}) \vee (\mathtt{k} = \mathtt{j} - 1) \vee (\mathtt{j} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}])$

$= \{\texttt{By domain split}\}$

$(\forall \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{b}[\mathtt{k}]) \wedge (\forall \mathtt{k} : \mathtt{k} = \mathtt{i} : \mathtt{b}[\mathtt{k}]) \wedge (\forall \mathtt{k} : \mathtt{k} = \mathtt{j} - 1 : \mathtt{b}[\mathtt{k}])$
$\wedge (\forall \mathtt{k} : \mathtt{j} \leq \mathtt{k} < \mathtt{n} : \mathtt{b}[\mathtt{k}])$

$= \{\texttt{By quantification over singleton domain}\}$

$(\forall \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{b}[\mathtt{k}]) \wedge \mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j} - 1] \wedge (\forall \mathtt{k} : \mathtt{j} \leq \mathtt{k} < \mathtt{n} : \mathtt{b}[\mathtt{k}])$

$= \{\texttt{By domain split}\}$

$\mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j} - 1] \wedge (\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i}) \vee (\mathtt{j} \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}])$

$= \{\texttt{By rewriting using PIC.3}\}$

$\mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j} - 1] \wedge \mathtt{r}$

$= \{\texttt{By rewriting using true consequence on PIC.7}\}$

$\mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j} - 1] \wedge \mathtt{T}$

$= \{\texttt{By basic equalities of boolean connectors}\}$

$\mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j} - 1]$

END ____

17 $\{\texttt{Conjunction on 16, 11 and 15}\}$

$(\mathtt{b}[\mathtt{i}] \wedge \mathtt{b}[\mathtt{j} - 1] = (\forall \mathtt{k} : (0 \leq \mathtt{k} < \mathtt{i} + 1) \vee (\mathtt{j} - 1 \leq \mathtt{k} < \mathtt{n}) : \mathtt{b}[\mathtt{k}]))$
$\wedge (0 \leq \mathtt{i} + 1 \leq \mathtt{n}) \wedge (0 \leq \mathtt{j} - 1 \leq \mathtt{n})$

18 $\{\texttt{Rewrite 17 with 2}\}$

Q

END ____

Finally, the proof of the "false consequence" rule used in subproof sp2 of proof PEC:

PROOF FalseConsequence

[A1:] $\neg \mathtt{P}$
[G1:] $\mathtt{P} = \mathtt{F}$

BEGIN ____

1 $\{\texttt{See subproof by contradiction spc}\}$

$\mathtt{P} = \mathtt{F}$

PROOF spc

[A1:] $\mathtt{P} = \mathtt{T}$

[G1:] F

BEGIN ____

1 $\{\texttt{True consequence on A1}\}$

P

2 $\{\texttt{Contradiction on FalseConsequence.A1 and 1}\}$

F

END ____

END ____