Example of a Worked-out Proof

Consider again this program

- Let 0≤n. This program checks if *all* elements of the segment a[0..n) are zero.

- {* 0≤n *}

```
    i := 0 ; r := true ;
    while  i<n  do  {  r := r /\ (a[i]=0)  ;  i++ }
```

{* ?? *}

Proof rule for loop (total correctness)

-

$\{^* \; g \wedge I \; ^*\} \quad S \quad \{^* \; I \; ^*\}$ // invariance

$I \wedge \neg g \Rightarrow Q$ // exit cond

$\{^* \; I \wedge g \; ^*\} \quad C{:=}m;\ S \quad \{^* \; m<C \; ^*\}$ // m decreasing

$I \wedge g \Rightarrow m > 0$ // m bounded below

$\{^* \; I \; ^*\}$ <u>while</u> g <u>do</u> S $\{^* \; Q \; ^*\}$

Formal spec, inv, and term. metric

- {* $0 \leq n$ *}

```
    i := 0 ; r := true ;
    while  i<n  do  {  r := r /\ (a[i]=0)  ;  i++ }
```

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

- Chosen invariant & termination metric:

  I : $\underbrace{(r = (\forall k : 0 \leq k < i : a[k]=0))}_{I_1} \wedge \underbrace{0 \leq i \leq n}_{I_2}$

  m : $n - i$

It comes down to proving these

- (Exit Condition) $I \wedge \neg g \Rightarrow Q$
- (Initialization Condition)
  {* given-pre-cond *} i := 0 ; r := **true** {* I *},

  Equivalently : given-pre-cond $\Rightarrow$ **wp** (i := 0 ; r := **true**) I
- (Invariance) $I \wedge g \Rightarrow$ **wp** body I
- (Termination Condition) $I \wedge g \Rightarrow$ **wp** (C:=m ; body) (m<C)
- (Termination Condition) $I \wedge g \Rightarrow$ m>0

Proof of the exit condition

- PROOF PEC
  [A1] $r = (\forall k : 0 \le k < i : a[k]=0)$ // I1
  [A2] $0 \le i \le n$ // I2
  [A3] $i \ge n$ // $\neg g$
  [G] $r = (\forall k : 0 \le k < n : a[k]=0)$

1. { A2 and A3 } $i = n$

2. { rewrite A1 with 1 } $r = (\forall k : 0 \le k < n : a[k]=0)$

   END

Proof of the initialization condition

- Calculate the **wp** first :

  wp (i := 0 ; r := **true**) I = ...

- PROOF Init

  [A1] $0 \le n$

  [G] (true = ($\forall$k : $0 \le k < 0$: a[k]=0)) /\ $0 \le 0 \le n$ // calculated wp

1. { $0 \le 0$, conjunction with A1 } $0 \le 0 \le n$
2. { see the eq. sub proof below } true = ($\forall$k : $0 \le k < 0$: a[k]=0)

   EQUATIONAL PROOF

   ($\forall$k : $0 \le k < 0$: a[k]=0)

   = { the domain is empty }

   ($\forall$k : false : a[k]=0)

   = {$\forall$ over empty domain }

   true

   END
3. { conjunction of 1 and 2 } G

Proof of the invariance condition

- We have to prove: $I \land g \Rightarrow$ **wp** body I
- Calculate the wp first:

  wp $(r := r \land (a[i]=0)\ ;\ i{+}{+})\ \ I\ =\ ....$

- Proof structure:

  PROOF PIC
  [A1] $r = (\forall k : 0 \le k < i : a[k]=0)$ // I1
  [A2] $0 \le i \le n$ // I2
  [A3] $i<n$ // g
  [G] .... here the wp you calculated above

Proof of the invariance condition

- PROOF PIC
  [A1] r = $(\forall k : 0 \leq k < i : a[k]=0)$
  [A2] $0 \leq i \leq n$
  [A3] $i < n$
  [G1] $r \wedge (a[i]=0) = (\forall k : 0 \leq k < i+1 : a[k]=0)$
  [G2] $0 \leq i+1 \leq n$

1. { follows from $0 \leq i$ in A2 } $0 \leq i+1$
2. { follows from A3 } $i+1 \leq n$
3. { see eq. subproof below } G1

   EQUATIONAL PROOF ---------------------------

   $(\forall k : 0 \leq k < i+1 : a[k]=0)$
   = { dom. merge , PIC.A2 }
   $(\forall k : 0 \leq k < i \vee k=i : a[k]=0)$
   = { $\forall$ domain-split }
   $(\forall k : 0 \leq k < i: a[k]=0) \wedge (\forall k : k=i : a[k]=0)$
   = { PIC.A1 }
   $r \wedge (\forall k : k=i : a[k]=0)$
   = { quant. over singleton }
   $r \wedge (a[i]=0)$
   END

4. { conjunction of 1,2,3} G

END

Proof that m decreases

- You have to prove: $I \wedge g \Rightarrow$ **wp** (C:=m ; body) (m<C)
- Calculate this first:

$$\textbf{wp}\ \ (C:=n\text{-}i\ ;\ r := r \wedge (a[i]=0)\ \ ;\ \ i\text{++}\ )\ \ \ (n\text{-}i<C)\ \ \ =\ \ ....$$

- PROOF PTC1

[A1] $r = (\forall k : 0 \leq k < i : a[k]=0)$ // I1

[A2] $0 \leq i \leq n$ // I2

[A3] $i<n$ // g

[G] $n-(i+1) < n-i$

1. { $x-1 < x$ } $n - i - 1 < n-i$
2. { rewriting 1 } $n - (i+1) < n-i$

END

Proof that m has a lower bound

- You have to prove: I /\ g $\Rightarrow$ m$\geq$0
- PROOF PTC2

  [A1] r = ($\forall$k : 0$\leq$k<i : a[k]=0) // I1

  [A2] 0$\leq$i$\leq$n // I2

  [A3] i<n // g

  [G] n – i > 0

  ..... complete this yourself.

Let's take a look at the version with a break

- $\{^*\ 0 \leq n\ ^*\}$

  let's call this $g \wedge h$

  $i := 0$; $r :=$ **true** ;
  while $i<n \wedge r$ **do** $\{\ r := r \wedge (a[i]=0)\ ;\ i\text{++}\ \}$

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

- Let's just use the same invariant & termination metric:

  $I\ :\ (r = (\forall k : 0 \leq k<i : a[k]=0))\ \wedge\ 0 \leq i \leq n$
  $m :\ n - i$

Ok.. so what do we have to prove ?

- (Exit Condition) $I \wedge \neg(g \wedge h) \Rightarrow Q$
- (Initialization Condition)
  given-pre-cond $\Rightarrow$ **wp** (i := 0 ; r := **true**) I
- (Invariance) $I \wedge g \wedge h \Rightarrow$ **wp** body I
- (Termination Condition) $I \wedge g \wedge h \Rightarrow$ **wp** (C:=m ; body) (m<C)
- (Termination Condition) $I \wedge g \wedge h \Rightarrow m>0$

Patched proof of the exit condition

- PROOF PEC
  [A1] $r = (\forall k : 0 \le k < i : a[k]=0)$ // I1
  [A2] $0 \le i \le n$ // I2
  [A3] $i \ge n \lor \neg r$ // $\neg g$
  [G] $r = (\forall k : 0 \le k < n : a[k]=0)$

1. { see subproof1} $i \ge n \Rightarrow G$
2. { see subproof2} $\neg r \Rightarrow G$
3. { case-split on A3, using 1 and 2 } G

END

The Subproofs of PEC

- PROOF sub2
  [A1] $\neg r$
  [G] $r = (\forall k : 0 \leq k < n : a[k]=0)$

1. { rewrite A1 with PEC.A1} $\neg(\forall k : 0 \leq k < i : a[k]=0)$
2. { neg of $\forall$ on 1 } $(\exists k : 0 \leq k < i : a[k] \neq 0)$
3. {$\exists$ elim on 2} **[SOME k]** $0 \leq k < i \wedge a[k] \neq 0$
4. {PEC.A2 says $i \leq n$, so 3 implies this: } $0 \leq k < n \wedge a[k] \neq 0$
5. {$\exists$ intro on 4 } $(\exists k : 0 \leq k < n : a[k] \neq 0)$
6. { neg of $\forall$ on 5 } $\neg(\forall k : 0 \leq k < n : a[k]=0)$
7. {A1 and 6 } $\neg r = \neg(\forall k : 0 \leq k < n : a[k]=0)$
8. { follows from 7 } $r = (\forall k : 0 \leq k < n : a[k]=0)$

   END

$$\frac{P \quad , \quad Q}{P = Q}$$

We can also prove sub2's goal with an equational proof

- EQ PROOF sub2
  [A1] $\neg r$

$(\forall k : 0 \le k < n : a[k]=0)$

= { domain merging, justified by PEC.A2 } $(\forall k : 0 \le k < i \lor i \le k < n : a[k]=0)$

= { domain split } $(\forall k : 0 \le k < i : a[k]=0) \land (\forall k : i \le k < n : a[k]=0)$

= { rewrite with PEC.A1 } $r \land (\forall k : i \le k < n : a[k]=0)$

= { rewrite with A1 above } $\text{false} \land (\forall k : i \le k < n : a[k]=0)$

= { trivial } false

= { A1 implies r=false } r

END