Pre-lecture Video

Program Correctedness

If the $\overbrace{\text{proper condition to run the program}}^{\text{Precondition}}$ holds, and the program is run, then the program $\underbrace{\text{will halt}}_{\text{termination}}$, and when it halts, the $\underbrace{\text{desired result}}_{\text{Post condition}}$ follows.

Pre + Post : Specification

In general, Precon ⇒ (Termination and Postcon)

Prove 2 parts (iterative code)

(i) Precon ⇒ Termination "Proving Termination"

(ii) (Precon and Termination) ⇒ Postcon "Proving Partial Correctness"

Corollary: (PWO)

Every (strictly) decreasing sequence of natural numbers is finite.

Loop Invariant (LI):

A statement that's true on entry to the loop, and after every iteration.

Special Induction for proving LI

Basis: Prove LI holds on entry to loop

IS: For any, if LI holds before the iteration, then LI holds after the iteration.

Ex 1:

Prove correctedness for the following program.

Pre: $n \in \mathbb{N}$

Post: Return n^2

```
SQ(n)
1.  S = 0 ; d = 1 ; i = 0
2.  while i < n :
3.        s = s+d
4.        d = d+2
5.        i = i+1
6.  return s
```

Trace: n=4

Iteration	s	d	i
0	0	1	0
1	1	3	1
2	4	5	2
3	9	7	3
4	16	9	4

Ex 1 Continued ...:

Step 1: Find an LI

(i) $s = i^2$ (ii) $d = 2i+1$ (iii) $0 \le i \le n$

Step 2: Prove LI

Basis: On entry to loop

$s = 0,\ i = 0,\ d = 1$

$s = i^2,\ d = 2i+1,\ 0 \le i \le n$

I.S: Consider an arbitrary iteration

Suppose LI holds before the iteration [IH]

WTP LI holds after the iteration.

$s' = s + d$ [Line 3] $i' = i+1$ [Line 5]

$= i^2 + 2i + 1$ [IH]

$= (i+1)^2$

$= i'^2$, as wanted

$d' = d + 2$ [Line 4]

$= (2i+1) + 2$ [IH]

$= 2(i+1) + 1$

$= 2i' + 1$, as wanted

$i < n$ [because of the while condition]

$\therefore\ 0 \le i < i+1 \le n$, as wanted

Step 3: Prove Partial Correctness (i.e. LI + exit condition $\Rightarrow$ Post condition)

Suppose loop terminates and consider the values of s, d, i on exit.

By LI(iii), $i \le n$

By exit condition, $i \ge n$

Hence $i = n$ (*)

By LI(i), $s = i^2$

$= n^2$ [*]

By line 6, $s = n^2$ is returned as wanted

Ex 1 Continued ...:

Step 4: Find expression e to associate with each iteration of loop.

$e = n - i$

WTS $e' = e - 1 < e$

Step 5: Prove $e \geq 0$ and e is strictly decreasing

By LI(iii), $i \leq n$ $\therefore$ $e = n - i \geq 0$

Consider an arbitrary iteration:

$$\begin{aligned} e' &= n - i' \\ &= n - (i+1) \quad [\text{Line } 5] \\ &= n - i - 1 \\ &= e - 1 < e \quad \text{as wanted} \end{aligned}$$

Ex 2:

Pre: $n \in \mathbb{N}$
Post: return n^2

```
SQ(n)
1.    if n = 0:
2.        result = 0
3.    else:
4.        result = SQ(n-1) + 2n - 1
5.    return result
```

General Form

$Q(k)$: if precon and $k =$ "input size", then program halts and postcon follows.
(i.e. the program is correct when input size is k.)

Then use PCI to prove $Q(k)$ holds for all valid values of k.

Proof:

$Q(k)$: If $n \in \mathbb{N}$ and $k = n$, then $SQ(n)$ halts and returns n^2

$Q(n)$: If $n \in \mathbb{N}$, then $Q(n)$ returns n^2

Use PCI to prove $Q(n)$ $\forall n \in \mathbb{N}$, then correctness follows.

Base cases: Let $n = 0$

$SQ(n)$ returns 0 [lines 1, 2, 5]
$\therefore$ $SQ(n)$ returns n^2, as wanted.

Ex 2 continued... :

Proof:

I.S.: Let $n > 0$

Suppose $Q(j)$ holds whenever $0 \leq j < n$ [I.H.]

WTP $Q(n)$ holds

Since $n > 0$, $SQ(n)$ runs line 4 [line 1]

Also, since $n > 0$, then $0 \leq n-1 < n$.

Hence I.H. applies to $SQ(n-1)$

By I.H., $SQ(n-1)$ returns $(n-1)^2$

By lines 4,5, $SQ(n)$ returns $(n-1)^2 + 2n - 1 = n^2 - 2n + 1 + 2n - 1$

$= n^2$, as wanted

B36 Sept 22 Lec 1 Notes

1a. $(0,1)$ and $(1,1)$
$= (0\cdot1 - 1\cdot1,\ 0\cdot1 + 1\cdot1)$
$= (-1, 1)$

$(-1, 1)$ and $(1,1)$
$= (-1\cdot1 - 1\cdot1,\ -1\cdot1 + 1\cdot1)$
$= (-2, 0)$

(x,y) and (v,w)
$(xv - yw,\ xw + yv)$

$(0,1)$ and $(-1,1)$
$= (0\cdot1 - 1\cdot1,\ 0\cdot1 + 1\cdot1)$
$= (-1, 1)$

$(-1,1)$ and $(-2,0)$
$= ((-1)(-2) - (1)(0),\ 1\cdot0 + 1(-2))$
$= (2, -2)$

$(2,-2)$ and $(-1,1)$
$= (2(-1) - (-2)(1),\ (2)(1) + (-2)(-1))$
$= (0, 0)$

$(4,0)$ and $(1,1)$
$= (4 - 0\cdot1,\ 4 + 0)$
$= (4,4)$

$(1,1)$ and $(2,-2)$
$= (1\cdot2 - 1(-2),\ 1(-2) + (1)(2))$
$= (4, 0)$

$H = \{ (s,t) \in \mathbb{Z}^n : s^2 + t^2 \text{ is a power of } 2 \}$

i.e. $(s,t) = (\pm 2^n, 0)$
$(s,t) = (0, \pm 2^n)$
$(s,t) = (\pm 2^n, \pm 2^n)$

1b. Prove for any (s,t) in G, (s,t) in H.

Proof:

$P(a,b): (a,b) \in H$ i.e. $a^2 + b^2$ is a power of 2

Base case: 2 cases, $(a,b) = (0,1)$; $(a,b) = (1,1)$

$(0,1)$ in G, $0^2 + 1^2 = 1 = 2^0$ in H
$(1,1)$ in G, $1^2 + 1^2 = 2 = 2^1$ in H

I.S: Let $(x,y), (v,w) \in G$
Suppose $P(x,y)$ and $P(v,w) \in H$
i.e. $(x^2+y^2) \in H$, $x^2+y^2 = 2^i$; $(v^2+w^2) \in H$, $v^2+w^2 = 2^j$ [I.H]

WTP $P(xv - yw, xw + yv)$

$= (xv - yw)^2 + (xw + yv)^2$
$= (xv)^2 - 2ywxv + (yw)^2 + [(xw)^2 + 2xwyv + (yv)^2]$
$= x^2v^2 + y^2w^2 + x^2w^2 + y^2v^2$
$= x^2(v^2 + w^2) + y^2(w^2 + v^2)$
$= (x^2 + y^2)(w^2 + v^2)$
$= (2^i)(2^j)$ [I.H]
$= 2^{i+j} \in H$, as wanted

1c. Prove $H \subseteq G$

Proof:

$P(k)$: $\forall a,b \in \mathbb{Z}$, if $a^2+b^2=2^k$, then $(a,b) \in G$