A2: - Friday office hour 4-6 in BA3201
- questions right now
- widespread misimpression that consecutive $\equiv$ 2

CSC236 fall 2016

correct after & before

Danny Heap
heap@cs.toronto.edu / BA4270 (behind elevators)
http://www.cdf.toronto.edu/~heap/236/F12/
416-978-5899

Using Introduction to the Theory of Computation, Chapter 2

Outline

power

notes

integer power

```
def power(x, y) :
  z = 1
  m = 0
  while m ≤ y :
    z = z * x
    m = m + 1
  return z
```

PRE

#3

POST

LI $z_i = x^{m_i}$

$\wedge \; m_i \leq y$

Prove LI using

- precondition? $y \in \mathbb{N}$, $x \in \mathbb{R}$, $z = 1$, m_0
- postcondition? $z = x^y$
- notation for mutation indicate state of variable after i iterations of loop by subscript i

So $z_0 = 1$, $m_0 = 0$ $\quad z_{i+1} = z_i * x$

$m_{i+1} = m_i + 1$

partial correctness

precondition+execution+termination imply postcondition

a loop invariant helps get us closer

① Prove that $\forall i \in \mathbb{N}$, $P(i)$ where $* \wedge m_i \in \mathbb{N}$

$P(i)$: $z_i = x^{m_i} \wedge m_i \leq y$ if there is an iteration i.

Base case $i=0$: $z_0 = 1 = x^0 = x^{m_0}$ ✓ $\wedge$ $m_0 = 0 \leq y \in \mathbb{N}$ $\wedge$ $m_0 = 0 \in \mathbb{N}$

So $P(0)$ is true.

Inductive step: Let $i \in \mathbb{N}$, assume $P(i)$ and assume that there is an $(i+1)$th loop iteration.

Then $z_{i+1} = z_i * x$ # by line ? of code.

$= x^{m_i} * x$ # by IH

$= x^{m_i + 1} = x^{m_{i+1}}$ # $m_{i+1} = m_i + 1$

Since there is an $(i+1)$th loop iteration we know $m_i < y \Rightarrow m_i + 1 = m_{i+1} \leq y$

$m_i \in \mathbb{N} \Rightarrow \underbrace{m_i + 1}_{= m_{i+1}} \in \mathbb{N}$ # $m_i, 1 \in \mathbb{N}$, closed under +

$\therefore P(i) \Rightarrow P(i+1)$

we've shown $\forall i \in \mathbb{N}$, $P(i)$

partial correctness

precondition+execution+termination imply postcondition

a loop invariant helps get us closer

LI (proved) says $z_i = x^{m_i}$ and $m_i \leq y$

after, say, f iteration & loop terminates

so $m_f \not< y \wedge m_f \leq y$ # by LI ∧ termination

$\Longrightarrow m_f = y$ so $z_f = x^{m_f}$ # by LI

$= x^y$

prove partial correctness

prove termination

associate a decreasing sequence in $\mathbb{N}$ with loop iterations

it helps to add claims to the loop invariant

Choose sequence $\langle y - m_i \rangle$ must show

① $\langle y - m_i \rangle \in \mathbb{N}$

② if iteration $i+1$ occurs.

$\langle y - m_i \rangle > \langle y - m_{i+1} \rangle$

① $y, m_i \in \mathbb{N}$ # Precondition $\wedge$ LI

$\Rightarrow y - m_i \in \mathbb{Z}$

also $m_i \leq y \Rightarrow 0 \leq y - m_i$

$\Rightarrow y - m_i \in \mathbb{N}$

② $y - m_i > y - m_i - 1 = y - (m_i + 1)$

$= y - m_{i+1}$

$\therefore \langle y - m_i \rangle$ is a strictly decreasing sequence in $\mathbb{N}$,

thus it has a smallest element, call it $\langle y - m_f \rangle$

$\therefore$ there are f iteration and no more

$\Rightarrow$ termination

put it together — correctness

① Partial correctness

PRE + LI + termination $\Rightarrow$ POST

② termination

$\therefore$ PRE $\Rightarrow$ POST.

correctness by design

draw pictures of before, during, after

pre: A sorted, comparable with x

post: $0 \leq p \leq n$ and $\underbrace{\text{A[0..p-1]}}_{\text{may be empty}} < x \leq \underbrace{\text{A[p .. n-1]}}_{\text{may be empty}}$

? compared to x

0 e n

b

Pre:
A is sorted, elements are comparable to x

$b = 0$, $e = n-1$

(possibly empty $< x$?   possibly empty $\geq x$

b e

```
while b <= e:
    m = (b+e)/2
    if A[m] < x:
        b = m+1
    else:
        e = m-1
```

possibly empty $< x$ $\geq x$ (possibly empty)

0   e b $n-1$

return b

Post

“derive” conditions from pictures

Pre A is sorted non-decreasing, elements are comparable to x. $|A| = n$. $b = 0$, $e = n-1$.

Post * $b \leq e+1 \leq n$. $\forall k, 0 \leq k \leq b-1$ $A[i] < x$
$\forall k, b \leq k \leq n-1$ $A[i] \geq x$

Loop Invariant: at the end of the ith loop iteration (if there is one): $\forall k, 0 \leq k \leq b_i - 1$, $A[k] < x$
$\forall k, e_i + 1 \leq k \leq n-1$, $A[k] \geq x$

$$0 \leq b_i \leq e_i + 1 \leq n \wedge b_i, e_i \in \mathbb{N}$$

* a better post: $\underline{\underline{0}} \leq b \leq e+1 \leq n$
– easy to add 0 – b LI + prove.

Prove Loop Invariant P(i): If there is an ith loop iteration at the end of it

- $\forall k,\ 0 \le k < b_i,\ A[k] < x$
- $\forall k,\ e_i+1 \le k < n,\ A[k] \ge x$
- $b_i \le e_i + 1 \le n$

base case By PRE $b_0 = 0,\ e_0 = n-1$

- there are no k st $0 \le k < 0 = b_0$
- there are no k st $e_0+1 = n \le k < n$

so these claims are vacuously true. also $b_0 = 0 \le e_0 + 1 = n \in \mathbb{N}$.

Inductive Step Let $i \in \mathbb{N}$. assume P(i). If there is an $(i+1)$th loop iteration, then:

$b_i \le e_i$ (loop condition)

$m = (b_i + b_i) // 2$ # integer division

Case $A[m] < x$:

$b_{i+1} = m+1$

$e_{i+1} = e_i$

by IH, $P(i)$ – $\forall k,\ e_{i+1} = e_i \leq k < n,\quad A[k] \geq x$

– $\forall k,\ 0 \leq k \leq b_{i+1} - 1 = m,\quad A[k] < x,$

Since $A[m] < x$ and A is sorted.

– $m = (b_i + e_i)//2 \Rightarrow m \leq 2 \cdot e_i // 2$

$\Rightarrow m \leq e_i \Rightarrow b_{i+1} = m+1 \leq e_i + 1 = e_{i+1} + 1$

$\leq n.$

Thus $P(i)$ holds in this case.

Case $A[m] \geq x$:

$e_{i+1} = m - 1,\quad b_{i+1} = b_i$

– by IH $P(i)$: $\forall k,\ 0 \leq k \leq b_i - 1 = b_{i+1} - 1\quad A[k] < x$

– Since $A[m] = A[e_{i+1} + 1] \geq x$ and A is sorted

$\forall k,\ e_{i+1} + 1 \leq k < n,\quad A[k] \geq x$

– $b_{i+1} = b_i = \frac{2b_i}{2} \leq \left\lfloor \frac{b_i + e_i}{2} \right\rfloor = m = e_{i+1} + 1 \leq e_i < n$

$\left(m \leq \frac{2e_i}{2} = e_i < n \text{ by IH} \right)$

$\longrightarrow$

Thus, in each possible case $P(i+1)$ follows from $P(i)$.

Partial Correctness

assume pre-condition an termination

$\Rightarrow e_f < b_f$ after final iteration f

$e_f + 1 \geq b_f$, by loop invariant.

$\Rightarrow e_f = b_f - 1$ (e + b are integers).

By loop invariant: $\forall k,\ 0 \leq k \leq b_f - 1,\ A[k] < X$

$\forall k,\ e_f + 1 = b_f \leq k < n,\ A[k] \geq X$

This is the post condition. $\wedge\ b_f \leq e_f + 1 \leq n$

<u>Termination</u> <u>Claim</u> $e_i + 1 - b_i \in \mathbb{N}$.

- By loop invariant $e_i + 1 \geq b_i \Rightarrow e_i + 1 - b_i \geq 0$

also $e, b, 1 \in \mathbb{Z}$, so $e_i + 1 - b_i \in \mathbb{Z}$

Thus $e_i + 1 - b_i \in \mathbb{N}$.

Suppose there is an $(i+1)$th iteration.

Then either:

- $e_{i+1} = e_i$ and $b_{i+1} = \left\lfloor \frac{b_i + e_i}{2} \right\rfloor + 1 > \frac{2b_i}{2} = b_i$

$$\Rightarrow e_{i+1} + 1 - b_{i+1} = e_i + 1 - b_{i+1} > e_i + 1 - b_i$$

- $e_{i+1} = \left\lfloor \frac{b_i + e_i}{2} \right\rfloor - 1 < \frac{2e_i}{e_i} = e_i \wedge b_{i+1} = b_i$

$$\Rightarrow e_{i+1} + 1 - b_{i+1} = e_{i+1} + 1 - b_i < e_i + 1 - b_i$$

In both cases $e_{i+1} + 1 - b_{i+1} < e_i + 1 - b_i$

$\therefore$ $e_i + 1 - b_i$ is a descending sequence in $\mathbb{N} \Rightarrow$ finite!