

- A2: - Friday office hour 4-6 in BA3201
- questions right now
- wide spread 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
```

PRE

```
    m = 0
```

```
    while m ≤ y :
```

```
        [ z = z * x ]  
        [ m = m + 1 ]
```

```
    return z
```

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 $z_0 = 1, m_0 = 0$

$$z_{i+1} = z_i * x$$
$$m_{i+1} = m_i + 1$$



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 $i=0$: $Z_0 = 1 = X^0 = X^{m_0} \checkmark \wedge m_0 = 0 \leq y \in \mathbb{N}$
So $P(0)$ is true. $m_0 = 0 \in \mathbb{N}$

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 $m_i < y \Rightarrow m_i + 1 = m_{i+1} \leq y$
 $m_i \in \mathbb{N} \Rightarrow m_i + 1 \in \mathbb{N} \# m_i, i \in \mathbb{N}$, closed under +
 $= m_{i+1}$

$\therefore P(i) \Rightarrow P(i+1)$
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, "iteration" & loop terminates

so $m_f \neq y \wedge m_f \leq y$ # by LI & termination

$\Rightarrow m_f = y$ 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

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

$$\text{also } m_i \leq y \Rightarrow 0 \leq y - m_i$$

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

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
 $PRE + LI + \text{termination} \Rightarrow POST$

② termination

$\circ \circ \quad PRE \Rightarrow POST.$



correctness by design

draw pictures of before, during, after

pre: A sorted, comparable with x

post: $0 \leq p \leq n$ and $A[0..p-1] < x \leq A[p..n-1]$

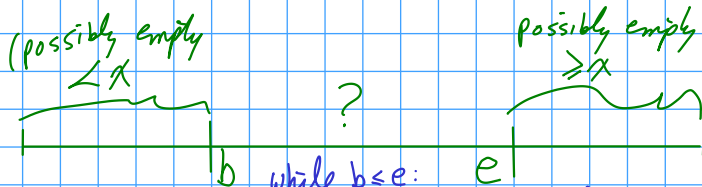
may be empty

may be empty

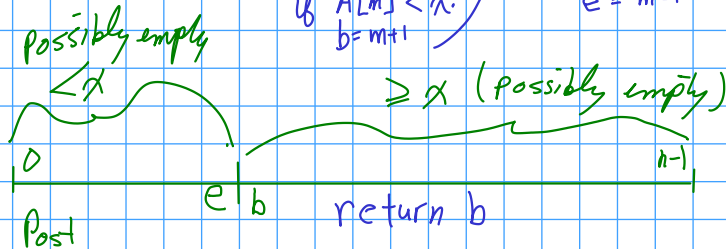


? compared to x

0 b Pre: A is sorted, $\uparrow$ elements are comparable to x e n
 $b=0, e=n-1$



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



"derive" conditions from pictures

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

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

Loop Invariant: at the end of the i th 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: $0 \leq b \leq e+1 \leq n$

- easy to add 0 to L + prove.



Prove Loop Invariant

$P(i)$: If there is an i th loop iteration at the end of it

$$- \forall k, 0 \leq k < b_i, A[k] < X$$

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

$$- b_i \leq e_{i+1} \leq n$$

base case

By PRE

$$b_0 = 0, e_0 = n-1$$

$$- \text{there are no } k \text{ st } 0 \leq k < 0 = b_0$$

$$- \text{there are no } k \text{ st } e_0 + 1 = n \leq k < n$$

so these claims are vacuously true. Also

$$b_0 = 0 \leq e_0 + 1 = n \in \mathbb{N}.$$

Inductive Step Let $i \in \mathbb{N}$. Assume $P(i)$. If there is

an $(i+1)$ th loop iteration, then:

$$b_i \leq e_i \text{ (loop condition)}$$

$$m = (b_i + e_i) // 2 \text{ \# integer division}$$

Case $A[m] < X$:

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

$$e_{i+1} = e_i$$



by IH, $P(i) - \forall k, e_{i+1} = e_i \leq k < n, A[k] \geq x$
 $- \forall k, 0 \leq k \leq b_{i+1} - 1 = m, A[k] < x$,
 Since $A[m] < x$ and A is sorted.

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

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

Thus $P(i)$ holds in this case. $\leq n$.

Case $A[m] \geq x$:

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

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

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

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

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

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



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

Partial Correctness

assume pre-condition and termination

$$\Rightarrow e_f < b_f \quad \text{after final iteration } f$$

$$e_{f+1} \geq b_f, \text{ by loop invariant.}$$

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

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. $\wedge b_f \leq e_{f+1} \leq n$



Termination Claim $e_{i+1} - b_i \in \mathbb{N}$.

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

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

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

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

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!