CSC236 fall 2012

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

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

- **precondition?** $x \in \mathbb{R}, y \in \mathbb{N}$
- **postcondition?** terminates, returns $x^y$, i.e., $z = x^y$
- **notation for mutation** let $Z_i$ and $m_i$ refer to values after $i$th iteration of loop (at lin 3) (loop has iterated $i$ times)
partial correctness

precondition + execution + termination imply postcondition

A loop invariant helps get us closer

\[ P(i) \quad \text{If there is an } i \text{th iteration of the loop, then } m_i \leq y, \forall i \in \mathbb{N}, Z_i = x^m_i \text{ and precondition satisfied} \]

Claim \[ \forall i \in \mathbb{N}, P(i) \]

Base case when \( i = 0 \) then \( m_i = 0, Z_i = 1, y \in \mathbb{N} \)

by precondition. Then \( m_i = 0 \leq y \in \mathbb{N} \) and \( Z_i = 1 = x^{m_i} = x^0 = 1 \). So \( P(0) \) holds.

Induction step Assume \( i \in \mathbb{N}, P(i) \) hold, and there is an \( (i+1) \text{th iteration} \),

Then, since loop condition succeeds, \( m_i < y \), so \( m_{i+1} \leq y \) \( (y \in \mathbb{N}) \Rightarrow m_{i+1} \leq y \). Also \( m_{i+1} \leq y \) \( (y \in \mathbb{N}) \Rightarrow M_{i+1} \leq y \). Also \( Z_{i+1} = Z_i \times x = x^{m_i} \times x^{(1)} = x^{m_{i+1}} \text{ (line 5)} \)

So, \( P(i+1) \) holds.
partial correctness
precondition + execution + termination imply postcondition
a loop invariant helps get us closer

Thus, whenever $P(i)$ true + there is an $(i+1)^{th}$ iteration, $P(i+1)$ follows.

Conclude $\forall i \in \mathbb{N}, P(i)$

if precondition is satisfied (+ execution)
+ program terminates

$\Rightarrow \exists ! m_k \leq y \land z_k = x^{m_k}$ for the
final index $k$.

also, since loop terminates $m_k \neq y$

$\Rightarrow m_k = y$ ($m_k \neq y \land m_k \leq y$).

$\Rightarrow z_k = x^{m_k} = x^y$.
prove partial correctness

see previous
prove termination
associate a decreasing sequence in $\mathbb{N}$ with loop iterations
it helps to add claims to the loop invariant

Show $\langle y - m_i \rangle$ is strictly decreasing in $\mathbb{N}$.

**Note** $y \in \mathbb{N}$, $m_i \in \mathbb{N}$ and $m_i \leq y \Rightarrow y - m_i \geq 0$,
so $y - m_i \in \mathbb{N}$.

**Claim** Assume there is an $(i+1)$th iteration of the loop. Then $y - m_i > y - m_{i+1}$

**Proof** If loop iterates $i+1$ times then
$m_{i+1} = m_i + 1$, so $y - m_i > y - m_{i-1} = y - (m_i + 1) = y - m_{i+1}$

**Conclude** $\langle y - m_i \rangle$ is strictly decreasing in $\mathbb{N} \Rightarrow$ loop terminates.
put it together — correctness
**Preconditions:**
A is sorted, comparable to \( \chi \), \(|A| = n\)

**Postconditions:**
\( 0 \leq p \leq n \), \( A[0..p-1] < \chi \leq A[p..n-1] \)

\[ b = 0 \]
\[ e = n-1 \]

\[ A[0..b-1] < \chi \ ? \] \[ \leq A[e+1..n-1] \]

\[ A \]
\[ 0 \]
\[ b \]
\[ e \]
\[ n-1 \]

\[ \text{while } b \leq e \]
\[ m = (b+e) / 2 \]
\[ \text{# show } b \leq m \leq e \]

\[ \text{if } A[m] < \chi : b = m+1, \text{ else } e = m-1 \]

\[ A \]
\[ 0 \]
\[ b \]
\[ p \]
\[ e \]
\[ n-1 \]

From this, can show 
\[ b \leq e+1 \leq n \] 
**add this in variant.**
“derive” conditions from pictures

\[ b = 0 \]
\[ e = n-1 \]

while \( b \leq e \):

\[ m = \lfloor \frac{b+e}{2} \rfloor \]  # integer division

if \( A[m] < x \):

\[ b = m + 1 \]

else:

\[ e = m - 1 \]

return \( b \)

need termination, so

show \( \langle e_i + 1 - b_i \rangle \) is in \( \mathbb{N} \) and
decreasing \( e_i + 1 - b_i \geq e_i + 1 - m_{i+1} \)  # since

versus \( e_i + 1 - (m_{i+1}) \)

\( e_i + 1 - b_i > m_{i-1} + 1 - b_i \quad e_i + 1 - b_i > e_i + 1 - (m_{i+1}) \)
do we have termination?