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

Computer Science
UNIVERSITY OF TORONTO

Outline

power

notes

integer power

$y - m_i$ is decreasing in $\mathbb{N}$.

```
  def power(x, y) :
1   z = 1
2   m = 0
3   while m < y :
4     z = z * x
5     m = m + 1
6   return z
```

L1 $z_i = x^{m_i} \wedge m_i \leq y$

$m_i \in \mathbb{N}$
$\mathbb{N}$ closed under $+$.

- 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 line 3) (loop has iterated i times)

partial correctness

precondition+execution+termination imply postcondition

a loop invariant helps get us closer

$P(i)$ If there is an ith iteration of the loop, then $m_i \le y \wedge z_i = x^{m_i}$ + precond 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 $m_i = 0 \le y \in \mathbb{N}$ 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 $(i+1)$th iteration.

Then, since loop condition succeeds, $m_i < y$, so $m_i + 1 \le y$ $(y \in \mathbb{N}) \Rightarrow m_{i+1} \le y$. Also

$z_{i+1} = z_i \times x = x^{m_i} * x$ (IH)

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

$\Rightarrow$ LI $m_K \leq y \wedge z_K = x^{m_K}$ for the final index K.

also, since loop terminates $m_K \not< y$

$\Rightarrow m_K = y \quad (m_K \not< y \wedge m_K \leq y)$.

$\Rightarrow z_K = x^{m_K} = x^y$

prove partial correctness

prove termination

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

it helps to add claims to the loop invariant

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 $y - m_i > y - m_i - 1$

$= y - (m_i + 1)$

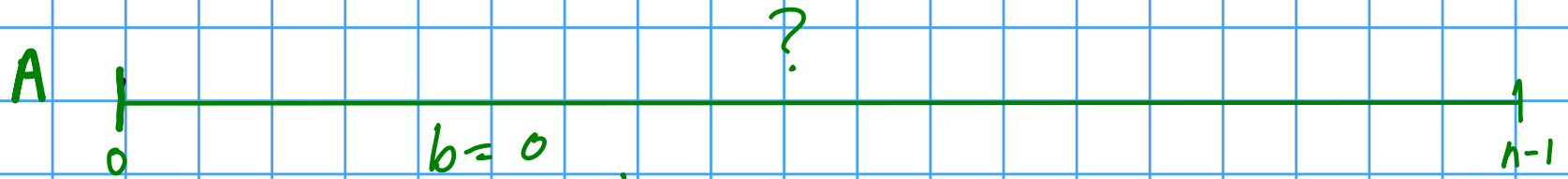
$= y - m_{i+1}$

Conclude $\langle y - m_i \rangle$ is strictly decreasing in $\mathbb{N}$. $\Rightarrow$ loop $\Rightarrow$ sequence is finite terminates.

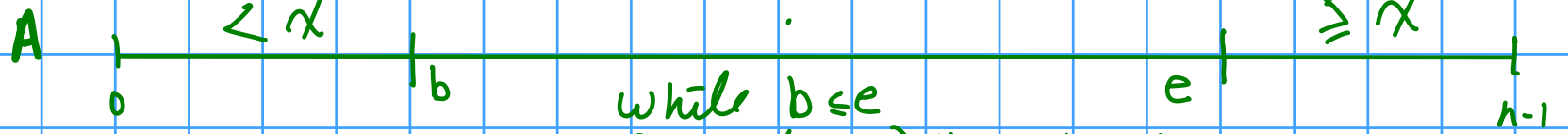
put it together — correctness

pre A is sorted ↑, comparable to x, |A| = n

post $0 \le p \le n$ $A[0..p-1] < x \le A[p..n-1]$



LI $A[0..b-1] < x \le A[e+1..n-1]$



while b ≤ e

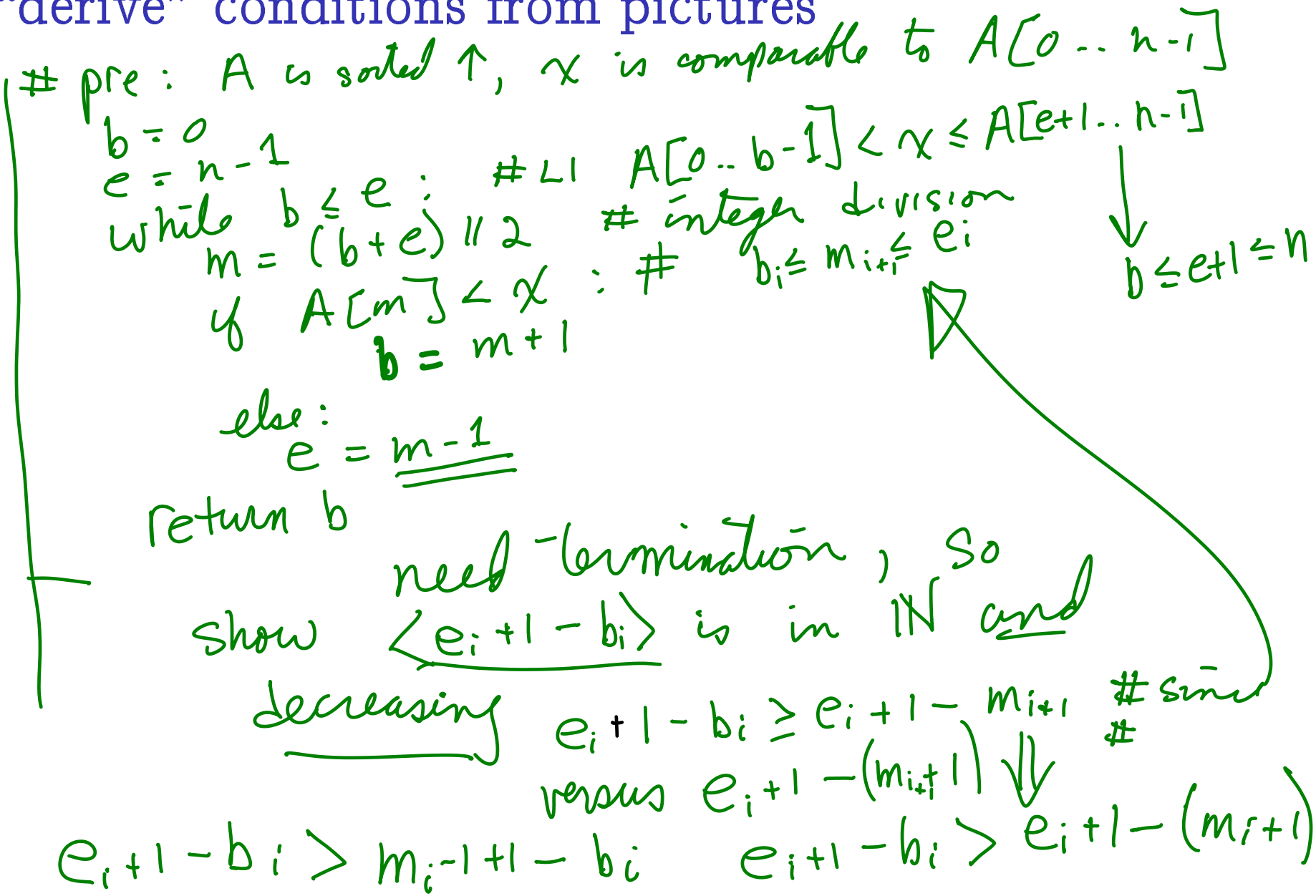
m = (b+e)//2 # show $b \le m \le e$

if A[m] < x: b = m+1, else e = m-1

A[a..b]

from this, can show $b \le e+1 \le n$ add this to loop invariant.

"derive" conditions from pictures



do we have termination?

notes