

CSC236 Homework Assignment #2

Induction Proofs on Program Correctness and
Recurrences

Alexander He Meng

Prepared for October 28, 2024

Question #1

Consider the following program from pg. 53-54 of the course textbook:

```
1 def avg(A):  
2     """  
3     Pre: A is a non-empty list  
4     Post: Returns the average of the numbers in A  
5     """  
6     sum = 0  
7     i = 0  
8     while i < len(A):  
9         sum += A[i]  
10        i += 1  
11    return sum / len(A)  
12  
13 print(avg([1, 2, 3, 4])) # Example usage
```

Denote the predicate:

$$Q(j) : \text{At the beginning of the } j^{\text{th}} \text{ iteration, } \text{sum}_j = \sum_{k=0}^{i_j-1} A[k].$$

Claim:

$$\forall j \in \{1, \dots, \text{len}(A)\}, Q(j)$$

Proof.

This proof leverages the Principle of Simple Induction.

Base Case:

Let $j = 1$.

At the beginning of the 1st iteration, $\text{sum}_1 = 0$ and $i_1 = 0$.

It follows that

$$\text{sum}_1 = \sum_{k=0}^{i_1-1} A[k] = \sum_{k=0}^{0-1} A[k] = \sum_{k=0}^{-1} A[k] = 0.$$

Hence, $Q(1)$.

Induction Hypothesis:

Assume for some iteration $m \in \{1, \dots, \text{len}(A) - 1\}$, $Q(m)$.

Namely, for the m^{th} iteration,

$$\text{sum}_m = \sum_{k=0}^{i_m-1} A[k].$$

Induction Step:

Proceed to show $Q(m+1)$:

Notice that $\text{sum}_{m+1} = \text{sum}_m + A[i_{m+1}]$, by *Line 9* of the program.

By the Induction Hypothesis,

$$\text{sum}_m + A[i_{m+1}] = \sum_{k=0}^{i_m-1} A[k] + A[i_{m+1}],$$

and by *Line 10* of the program, $i_{m+1} = i_m + 1$;

$$\sum_{k=0}^{i_m-1} A[k] + A[i_{m+1}] = \sum_{k=0}^{i_{m+1}-1} A[k].$$

Thus,

$$\text{sum}_{m+1} = \sum_{k=0}^{i_{m+1}-1} A[k]$$

as needed.

Therefore, by the Principle of Simple Induction, $Q(j)$ holds for all $j \in \{1, \dots, \text{len}(A)\}$.



Question #2

Recall $Q(j)$ from *Question # 1*:

$$Q(j) : \text{At the beginning of the } j^{\text{th}} \text{ iteration, } \text{sum}_j = \sum_{k=0}^{i_j-1} A[k].$$

Denote the following predicate:

$$Q'(n) : 0 \leq n < \text{len}(A) \implies Q(n+1)$$

Claim:

Proving $\forall j \in \{1, \dots, \text{len}(A)\}, Q(j)$ is equivalent to proving $\forall n \in \mathbb{N}, Q'(n)$.

Proof.

Remarks

It is sufficient to show that $\forall j \in \{1, \dots, \text{len}(A)\}, Q(j) \iff \forall n \in \mathbb{N}, Q'(n)$, to show that proving one of these statements is equivalent to proving the other.

$$(\forall j \in \{1, \dots, \text{len}(A)\}, Q(j)) \implies (\forall n \in \mathbb{N}, Q'(n)):$$

Suppose $\forall j \in \{1, \dots, \text{len}(A)\}, Q(j)$.

Then, fix $n \in \mathbb{N}$ and suppose $0 \leq n < \text{len}(A)$.

Because $n \in \{0, \dots, \text{len}(A) - 1\}$, it follows that $(n+1) \in \{1, \dots, \text{len}(A)\}$.

By assumption, $Q(n+1)$.

Thus, $\forall n \in \mathbb{N}, Q'(n)$.

$$(\forall j \in \{1, \dots, \text{len}(A)\}, Q(j)) \longleftarrow (\forall n \in \mathbb{N}, Q'(n)):$$

Suppose $\forall n \in \mathbb{N}, Q'(n)$.

Let $j \in \{1, \dots, \text{len}(A)\}$.

Then, $(j - 1) \in \mathbb{N}$.

It follows that $0 \leq j - 1 \leq \text{len}(A) - 1$.

Since $\text{len}(A) - 1 < \text{len}(A)$, $0 \leq j - 1 < \text{len}(A)$.

By assumption, $Q((j - 1) + 1)$.

Thus, $\forall j \in \{1, \dots, \text{len}(A)\}, Q(j)$.

Conclusion:

Therefore, $\forall j \in \{1, \dots, \text{len}(A)\}, Q(j) \iff \forall j \in \mathbb{N}, Q'(j)$.

□

Question #3

As follows below, Q6-Q10 respectively represent questions 6 through 10 from pp. 64-66 of the course textbook.

Q6:

Consider the following code:

```
1 def f(x):  
2     """Pre: x is a natural number"""  
3     a = x  
4     y = 10  
5     while a > 0:  
6         a -= y  
7         y -= 1  
8     return a * y
```

(a): Loop Invariant Which Characterizes a and y:

For arbitrary natural n...

Let $i_1 = 0$ and $i_n = i_{n-1} + 1$.

Let y_n be the value of y before the $(n + 1)$ th iteration. By *Line 4* (initializes $y = 10$) and *Line 7* (decrements y by 1) of the program, $y_n = 10 - \sum_{q=1}^n 1 = 10 - n \times 1 = 10 - n$.

Denote the loop invariant:

$$P(j) : (a_j = x - \sum_{k=0}^{i_j-1} y_k) \wedge (y_j = 10 - j)$$

For example, before the 1st iteration, $a_1 = x - \sum_{k=0}^{i_1-1} y_k = x - \sum_{k=0}^{0-1} y_k = x - 0 = x$.

Before the 2nd iteration, $a_2 = x - \sum_{k=0}^{i_2-1} y_k = x - \sum_{k=0}^{1-1} y_k = x - y_0 = x - 10$.

(b): Why This Function Fails to Terminate

Suppose $x > \sum_{k=1}^{10} k = 55$.

By $P(j)$, before the 11th iteration, $a_{11} = x - \sum_{k=0}^{i_{11}-1} y_k = x - \sum_{k=0}^{10-1} y_k = x - \sum_{k=0}^9 (10 - k) =$

$$x - [10 \sum_{k=0}^9 (1) - \sum_{k=0}^9 (k)] = x - [10(10) - \frac{9(9+1)}{2}] = x - [100 - 45] = x - 55.$$

Since $x > 55$, it follows that $a_{11} = x - 55 > 0$.

As well, y_{10} (the value of y after the 11th iteration) is $10 - 11 = -1$.

Notice that in all subsequent iterations, a will decrement by $y_n < 0|_{n \geq 11}$ (where n is the iteration number of the corresponding iteration).

Since a decrements by a negative number subsequently, the loop causes a to grow large, thereby retaining $a > 0$.

Thus, the function fails to terminate for $x > 55$ (because $\neg(a > 0)$ is never satisfied).

Q7:

(a) Consider the recursive program below:

```
1 def exp_rec(a, b):  
2     if b == 0:  
3         return 1  
4     else if b mod 2 == 0:  
5         x = exp_rec(a, b / 2)  
6         return x * x  
7     else:  
8         x = exp_rec(a, (b - 1) / 2)  
9         return x * x * a
```

Preconditions:

$$(b \in \mathbb{N}) \wedge (a \neq 0)$$

Postconditions:

Returns a^b .

Denote the following predicate:

$P(b)$: The program returns a^b .

Claim: $\forall b \in \mathbb{N}, P(b)$

Proof.

This proof explores the Principle of Complete Induction on b .

Fix $a \neq 0$.

Base Case:

Let $b = 0$.

Then, by *Lines 2-3* of the program, the program returns $1 = a^0 = a^b$.

Hence, $P(0)$.

Induction Hypothesis:

Assume for some $k \in \mathbb{N}$ and for all $l \in [0, k] \cap \mathbb{N}$, $P(l)$.

This means the program returns a^l for every l as described.

Induction Step:

Proceed to show $P(k + 1)$ with case analysis:

Case 1 - Suppose $(k + 1)(\text{mod } 2) \neq 0$:

Then, program again enters the **else** statement in *Line 7*.

Here, the program sets x to `exp_rec(a, ((k + 1) - 1) / 2)`.

Notice that `exp_rec(a, ((k + 1) - 1) / 2) = exp_rec(a, (k / 2))`.

Since $(k + 1)(\text{mod } 2) \not\equiv 0$, it must be that $k(\text{mod } 2 \equiv 0)$.

Thus, $\frac{k}{2} \in \mathbb{N}$ and $\frac{k}{2} < k$.

By the Induction Hypothesis, `exp_rec(a, k / 2)` returns $a^{\frac{k}{2}}$.

Finally, the original function call returns $x \times x \times a$, which evaluates to $a^{\frac{k}{2}} \times a^{\frac{k}{2}} \times a = a^{\frac{k}{2} + \frac{k}{2} + 1} = a^{k+1}$, as needed.

Thus, $P(k + 1)$ holds.

Case 2 - Suppose $(k + 1)(\text{mod } 2) \equiv 0$:

Then, the program reaches *Line 5* and sets x to `exp_rec(a, (k + 1) / 2)`.

Notice that $\frac{k+1}{2} \in \mathbb{N}$ and $\frac{k+1}{2} \leq k$.

By the Induction Hypothesis, `exp_rec(a, (k + 1) / 2)` returns $a^{\frac{k+1}{2}}$.

Finally, the original function call returns $x \times x$, evaluating to $a^{\frac{k+1}{2}} \times a^{\frac{k+1}{2}} = a^{\frac{k+1}{2} + \frac{k+1}{2}} = a^{k+1}$, as needed.

Thus, $P(k + 1)$ holds.

Conclusion:

Therefore, $P(k + 1)$ holds in all cases.

By the Principle of Complete Induction, $\forall b \in \mathbb{N}, P(b)$.

□

(b) Consider the iterative version of the previous program:

```
1 def exp_iter(a, b):  
2     ans = 1
```

```
3   mult = a
4   exp = b
5   while exp > 0:
6       if exp mod 2 == 1:
7           ans *= mult
8       mult = mult * mult
9       exp = exp // 2
10  return ans
```

Preconditions:

$$(b \in \mathbb{N}) \wedge (a \neq 0)$$

Postconditions:

Returns a^b .

Denote the following predicate:

$$P(i) : a^b = \text{mult}_i^{\text{exp}_i} \times \text{ans}_i$$

Claim: $(\forall b \in \mathbb{N})(\forall i \in [0, b] \cap \mathbb{N})(P(i))$ and the program terminates.

Proof.

Loop Invariant Proof:

To prove the loop invariant, this proof explores the Principle of Simple Induction on i .

Base Case:

Fix $b \in \mathbb{N}$. Let $i = 0$.

Then, the program retains the values $\text{mult}_0 = a$, $\text{exp}_0 = b$, and $\text{ans}_0 = 1$, and does not enter the loop.

Notice that $a^b = a^b \times 1 = \text{mult}_0^{\text{exp}_0} \times \text{ans}_0$.

Hence, $P(0)$.

Induction Hypothesis:

Assume for some $k \in \mathbb{N}$, $P(k)$;

$$P(k) : (a^b = \text{mult}_k^{\text{exp}_k} \times \text{ans}_k).$$

Induction Step:

Suppose $\text{exp}_{k+1} > 0$, so the following iteration runs.

Then, the program yields the following values:

$$\begin{cases} \text{mult}_{k+1} = \text{mult}_k \times \text{mult}_k = \text{mult}_k^2, & \text{by Line 8} \\ \text{exp}_{k+1} = \lfloor \frac{\text{exp}_k}{2} \rfloor, & \text{by Line 9} \end{cases}$$

Notice that $\text{mult}_{k+1}^{\text{exp}_{k+1}} = (\text{mult}_k^2)^{\lfloor \frac{\text{exp}_k}{2} \rfloor} = \text{mult}_k^{2 \lfloor \frac{\text{exp}_k}{2} \rfloor}$.

Proceed to show $P(k+1)$ with case analysis:

Case 1 - Suppose $\text{exp}_k(\text{mod } 2) \equiv 1$:

By Lines 6-7 of the program, $\text{ans}_{k+1} = \text{ans}_k \times \text{mult}_k$.

So, $(\text{mult}_{k+1}^{\text{exp}_{k+1}}) \times (\text{ans}_{k+1}) = (\text{mult}_k^{2 \lfloor \frac{\text{exp}_k}{2} \rfloor}) \times (\text{ans}_k \times \text{mult}_k)$.

Since $\text{exp}_k(\text{mod } 2) \equiv 1$, it follows that $2 \lfloor \frac{\text{exp}_k}{2} \rfloor = 2(\frac{\text{exp}_k-1}{2}) = \text{exp}_k - 1$.

Thus,

$$\begin{aligned} (\text{mult}_k^{2 \lfloor \frac{\text{exp}_k}{2} \rfloor}) \times (\text{ans}_k \times \text{mult}_k) &= (\text{mult}_k^{\text{exp}_k-1}) \times (\text{mult}_k \times \text{ans}_k) \\ &= \text{mult}_k^{\text{exp}_k-1} \times \text{mult}_k \times \text{ans}_k \\ &= (\text{mult}_k^{\text{exp}_k-1} \times \text{mult}_k) \times \text{ans}_k \\ &= (\text{mult}_k^{(\text{exp}_k-1)+1}) \times \text{ans}_k \\ &= \text{mult}_k^{\text{exp}_k} \times \text{ans}_k \\ &= a^b, \end{aligned}$$

by the Induction Hypothesis.

Therefore, $(\text{mult}_{k+1}^{\text{exp}_{k+1}}) \times (\text{ans}_{k+1}) = a^b$; $P(k+1)$ holds.

Case 2 - Suppose $\text{exp}_k(\text{mod } 2) \not\equiv 1$:

By *Line 6* of the program, *Line 7* does not run.

Hence, ans_{k+1} retains the value as represented by ans_k ; $\text{ans}_{k+1} = \text{ans}_k$.

So, $(\text{mult}_{k+1}^{\text{exp}_{k+1}}) \times (\text{ans}_{k+1}) = (\text{mult}_k^{2\lfloor \frac{\text{exp}_k}{2} \rfloor}) \times \text{ans}_k$.

Notice that $\text{exp}_k(\text{mod } 2) \not\equiv 1 \iff \text{exp}_k(\text{mod } 2) \equiv 0$.

So, $2\lfloor \frac{\text{exp}_k}{2} \rfloor = 2(\frac{\text{exp}_k}{2}) = \text{exp}_k$.

Then, it follows that $(\text{mult}_k^{2\lfloor \frac{\text{exp}_k}{2} \rfloor}) \times \text{ans}_k = (\text{mult}_k^{\text{exp}_k}) \times \text{ans}_k = a^b$, by the Induction Hypothesis.

Still, $(\text{mult}_{k+1}^{\text{exp}_{k+1}}) \times (\text{ans}_{k+1}) = a^b$; $P(k+1)$ likewise holds.

Conclusion of Loop Invariant:

Collectively, $P(k+1)$ holds in all cases.

By the Principle of Simple Induction, $(\forall b \in \mathbb{N})(\forall i \in [0, b] \cap \mathbb{N})(P(i))$.

Program Termination Proof

Notice that *Line 9* of the program performs floor division by 2 on exp in each iteration.

From continual division, exp eventually becomes small enough that it reaches 0 through the next floor division by 2.

Since the program's loop requires $\text{exp} > 0$ to run, having exp reach 0 indeed terminates the loop.

Conclusion:

Therefore, this program is both correct (by the loop invariant) and terminates.

□

Q8

Consider the following linear time program:

```
1  def majority(A):
2      """
3      Pre: A is a list with more than half its entries equal to x
4      Post: Returns the majority element x
5      """
6      c = 1
7      m = A[0]
8      i = 1
9      while i <= len(a) - 1:
10         if c == 0:
11             m = A[i]
12             c = 1
13         else if A[i] == m:
14             c += 1
15         else:
16             c -= 1
17         i += 1
18     return m
```

Denote the following predicate:

$P(n) : \text{somethinghere}$

Claim: expresshowthisiscorrect

Proof.

wordsgohere

□

Q9

Consider the bubblesort algorithm as follows:

```
1  def bubblesort(L):
2      """
3      Pre: L is a list of numbers
4      Post: L is sorted
5      """
6      k = 0
7      while k < len(L):
8          i = 0
9          while i < len(L) - k - 1:
10             if L[i] > L[i + 1]:
11                 swap L[i] and L[i + 1]
12             i += 1
13         k += 1
```

(a): Denote the inner loop's invariant:

$P(n) : \text{something here}$

Claim: prove inner loop

Proof.

words go here

□

(b): Denote the outer loop's invariant:

$P(n) : \text{something here}$

Claim: prove outer loop

Proof.

wordsgohere

□

(c): Denote the following predicate:

$$P(n) : \text{somethinghere}$$

Claim: expresshowthisiscorrect

Proof.

wordsgohere

□

Q10

Consider the following generalization of the `min` function:

```
1  def extract(A, k):
2      pivot = A[0]
3      # Use partition from quicksort
4      L, G = partition(A[1, ..., len(A) - 1], pivot)
5      if len(L) == k - 1:
6          return pivot
7      else if len(L) >= k:
8          return extract(L, k)
9      else:
10         return extract(G, k - len(L) - 1)
```

(a): Proof of Correctness

$$P(n) : \text{somethinghere}$$

Claim: proofofcorrectnessclaim

Proof.

wordsgohere

□

(b): Worst-Case Runtime
wordsgohere

Question #4

As follows below, VI, VII, X, XII, and XIV respectively represent questions 6, 7, 10, 12, and 14 from pp. 46-48 of the course textbook.

VI

Let $T(n)$ be the number of binary strings of length n in which there are no consecutive 1's. So, $T(0) = 1, T(1) = 2, T(2) = 3, \dots$, etc.

(a): Recurrence for $T(n)$:

recurrencehere

(b): Closed Form Expression for $T(n)$:

closedformhere

(c): Proof of Correctness of Closed Form Expression

Denote the following predicate:

$$P(n) : \text{somethinghere}$$

Claim: expresshowthisisincorrect

Proof.

wordsgohere

□

VII

Let $T(n)$ denote the number of distinct full binary trees with n nodes. For example, $T(1) = 1$, $T(3) = 1$, and $T(7) = 5$. Note that every full binary tree has an odd number of nodes.

Recurrence for $T(n)$:

recurrencehere

$$P(n) : \text{somethinghere}$$

Claim: $T(n) \geq \left(\frac{1}{n}\right)(2)^{(n-1)/2}$

Proof.

wordsgohere

□

X

A *block* in a binary string is a maximal substring consisting of the same symbol. For example, the string 0100011 has four blocks: 0, 1, 000, and 11. Let $H(n)$ denote the number of binary strings of length n that have no odd length blocks of 1's. For example, $H(4) = 5$:

0000 1100 0110 0011 1111

Recursive Function for $H(n)$:

$P(n) : \text{somethinghere}$

Claim: proveouterloop

Proof.

wordsgohere

□

Closed Form for H (Using Repeated Substitution):

XII

Consider the following function:

```
1  def fast_rec_mult(x, y):
2  n = length of x  # Assume x and y have the same length
3  if n == 1:
4      return x * y
5  else:
6      a = x // 10^(n // 2)
```

```
7      b = x % 10^(n // 2)
8      c = y // 10^(n // 2)
9      d = y % 10^(n // 2)
10     p = fast_rec_mult(a + b, c + d)
11     r = fast_rec_mult(a, c)
12     u = fast_rec_mult(b, d)
13
14     return r * 10^n + (p - r + u) * 10^(n // 2) + u
```

Worst-Case Runtime Analysis:

wordsgohere

XIV

Recall the recurrence for the worst-case runtime of quicksort:

$$\begin{cases} c, & \text{if } n \leq 1; \\ T(|L|) + T(|G|) + dn, & \text{if } n > 1. \end{cases}$$

where L and G are the partitions of the list.

For simplicity, ignore that each list has size $\frac{n-1}{2}$.

(a): Assume the lists are always evenly split; that is, $|L| = |G| = \frac{n}{2}$ at each recursive call.

Tight Asymptotic Bound on the Runtime of Quicksort:

determinehere

(b): Assume the lists are always very unevenly split; that is, $|L| = n - 2$ and $|G| = 1$ at each recursive call.

Tight Asymptotic Bound on the Runtime of Quicksort:

determinehere