

COMP 681 Formal Methods Spring 2008 Recitation 16—Solutions

1. The following algorithm takes an array A (say, of characters) and returns `true` if the contents of the array form a palindrome, that is, if they read the same left to right as right to left; otherwise, it returns `false`. Examples of palindromes include (excluding blanks and commas and ignoring case differences) “civic” and “a man, a plan, a canal, Panama”. Prove the correctness of this algorithm using weak induction. Be sure to attach the appropriate assertions.

```
PALINDROM(A)
1  left ← 1
2  right ← LENGTH[A]
3  while left < right
4      do if A[left] ≠ A[right]
5          then return false
6          left ← left + 1
7          right ← right - 1
8  return true
```

Answer

The following is the above algorithm with assertions added. We use n as shorthand for $\text{LENGTH}[A]$.

```
PALINDROM(A)
1  left ← 1
2  right ← LENGTH[A]
3  while left < right ▶ left-1 = n-right and
                         $\forall i \in \{1, \dots, \text{left}-1\} \bullet A[i] = A[n-i+1]$ 
4      do if A[left] ≠ A[right]
5          then return false ▶
                         $\exists i \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[i] \neq A[n-i+1]$ 
6          left ← left + 1
7          right ← right - 1
8  return true ▶ (if  $n$  is even, then left = right+1) and
                (if  $n$  is odd, then left = right) and
                 $\forall i \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[i] = A[n-i+1]$ 
```

Note that the assertion in line 3 is the negation of the last conjunct in the assertion in line 8.

We first prove the first two conjuncts of the assertion at line 8:

At line 8, (if n is even, then $\text{left} = \text{right}+1$) and (if n is odd, then $\text{left} = \text{right}$)

Proof

Since the loop terminates, at line 8, the negation of the loop condition must be true. So, at line 8,

$$\text{left} \geq \text{right} \quad (1)$$

If $n=1$ (so n is odd), then the loop is never executed and, at line 8, because of lines 1 and 2, $\text{left} = \text{right}$, and the statement holds. The remainder of the proof assumes that $n > 1$.

Since the loop was executed a previous time during which left was incremented (line 5) and right decremented (line 6), we have

$$\text{left}-1 < \text{right}+1 \quad (2)$$

From (1) and (2),

$$\text{left} < \text{right}+2 \leq \text{left}+2$$

or

$$\text{left}-2 < \text{right} \leq \text{left}$$

From this it follows that

$$\text{right} = \text{left} \text{ or } \text{right} = \text{left}-1 \quad (3)$$

From the assertion at line 3 (which is true at line 8 since execution goes from line 3 directly to line 8),

$$\text{left} = n - \text{right} + 1 \quad (4)$$

If $\text{right} = \text{left}$, then (4) reduces to $\text{left} = (n+1)/2$, which requires n to be odd. Thus, if n is odd, we have $\text{left} = \text{right}$. If $\text{right} = \text{left}-1$, then (4) reduces to $\text{left} = n/2 + 1$, which requires n to be even. Thus, if n is even, we have $\text{left} = \text{right}+1$. Since by (3) these are the only two ways left and right may be related, at line 8, the result holds.

We next prove the last conjunct in the assertion at line 8:

At line 8, $\forall i \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[i] = A[n-i+1]$.

Proof

We consider two cases, depending on whether n is even or odd.

Case n is even:

By the previous result and the case assumption,

$$\text{left} = \text{right}+1 \quad (4)$$

From the assertion at line 3,

$$\text{right} = n - \text{left} + 1$$

From this and (1),

$$\text{left} = n - \text{left} + 1 + 1$$

or

$$\text{left} = n/2 + 1 \quad (5)$$

Again from the assertion at line 3,

$$\forall i \in \{1, \dots, \text{left} - 1\} \bullet A[i] = A[n - i + 1]$$

From this and (5),

$$\forall i \in \{1, \dots, n/2\} \bullet A[i] = A[n - i + 1] \quad (6)$$

Since n is even,

$$n/2 = \lfloor n/2 \rfloor$$

From this and (6),

$$\forall i \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[i] = A[n - i + 1]$$

as required.

Case n is odd:

By the case assumption and the previous result,

$$\text{left} = \text{right} \quad (7)$$

From the assertion at line 3,

$$\text{right} = n - \text{left} + 1$$

From this and (7),

$$\text{left} = n - \text{left} + 1$$

or

$$\text{left} = (n+1)/2 \quad (8)$$

Again from the assertion at line 3,

$$\forall i \in \{1, \dots, \text{left} - 1\} \bullet A[i] = A[n - i + 1]$$

From this and (8),

$$\forall i \in \{1, \dots, (n-1)/2\} \bullet A[i] = A[n - i + 1] \quad (9)$$

Since n is odd,

$$(n-1)/2 = \lfloor n/2 \rfloor$$

From this and (9),

$$\forall i \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[i] = A[n - i + 1] \quad \text{Q.E.D.}$$

This completes the proof of the assertion at line 8.

Next, we prove the assertion at line 5:

$$\text{At line 5, } \exists i \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[i] \neq A[n - i + 1]$$

Proof

From the while condition,

$$\text{left} < \text{right} \quad (10)$$

From the assertion in line 3,

$$\text{right} = n - \text{left} + 1 \quad (11)$$

From this and (10),

$$\text{left} < n - \text{left} + 1$$

or

$$\text{left} < (n+1)/2$$

Thus,

$$\text{left} \leq \lfloor n/2 \rfloor$$

with equality possibly holding only when n is odd. From this, the fact that $\text{left} = 1$ when the loop is first encountered, the fact that left is only incremented in the loop, and the condition in line 4, it follows that, at line 5,

$$\exists \text{left} \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[\text{left}] \neq A[\text{right}]$$

By this and (11),

$$\exists \text{left} \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[\text{left}] \neq A[n-\text{left}+1]$$

Changing the bound variable to i , at line 5,

$$\exists i \in \{1, \dots, \lfloor n/2 \rfloor\} \bullet A[i] \neq A[n-i+1] \quad \text{Q.E.D.}$$

We now prove the assertion at line 3,

$$\text{At line 3, } \text{left}-1 = n-\text{right} \text{ and } \forall i \in \{1, \dots, \text{left}-1\} \bullet A[i] = A[n-i+1]$$

We prove this by weak induction on the value of left .

Proof

Basis: $\text{left} = 1$

Then line 3 is encountered for the first time. By line 1,

$$\text{left} = 1 \tag{12}$$

and, by line 2,

$$\text{right} = n$$

So $\text{left}-1 = 1-1 = 0$ and $n-\text{right} = n-n = 0$, hence

$$\text{left}-1 = n-\text{right},$$

establishing the first conjunct.

Now, trivially,

$$\forall i \in \emptyset \bullet A[i] = A[n-i+1] \tag{13}$$

By (12),

$$\{1, \dots, \text{left}-1\} = \{1, \dots, 0\} = \emptyset$$

By this and (13),

$$\forall i \in \{1, \dots, \text{left}-1\} \bullet A[i] = A[n-i+1],$$

establishing the second conjunct.

Induction step

Regarding terminology, we use left' to denote the value of the program variable left when execution reaches the top of the loop the k^{th} time and left (without decoration) to denote the value of program variable left the next time execution reaches the top of the loop. We use right' and right similarly.

Now, assume that

$$\text{left}'-1 = n-\text{right}' \text{ and } \forall i \in \{1, \dots, \text{left}'-1\} \bullet A[i] = A[n-i+1]$$

(and show that

$$\text{left}-1 = n-\text{right} \text{ and } \forall i \in \{1, \dots, \text{left}-1\} \bullet A[i] = A[n-i+1]).$$

Since we assume that execution reaches line 3 again after executing the body with the values left' and right' for the corresponding program variables, the condition in line 4 with these values was false, so

$$A[\text{left}'] = A[\text{right}'] \quad (14)$$

By line 6,

$$\text{left} = \text{left}' + 1$$

or

$$\text{left}' = \text{left} - 1 \quad (15)$$

By line 7,

$$\text{right} = \text{right}' - 1$$

or

$$\text{right}' = \text{right} + 1 \quad (16)$$

By the induction hypothesis,

$$\text{left}' - 1 = n - \text{right}' \quad (17)$$

Substituting with (15) and (16),

$$\text{left} - 1 - 1 = n - \text{right} - 1$$

or

$$\text{left} - 1 = n - \text{right} \quad (18)$$

Also by the induction hypothesis,

$$\forall i \in \{1, \dots, \text{left}' - 1\} \bullet A[i] = A[n - i + 1] \quad (19)$$

From (14) and (17),

$$A[\text{left}'] = A[n - \text{left}' + 1]$$

From this and (19),

$$\forall i \in \{1, \dots, \text{left}'\} \bullet A[i] = A[n - i + 1]$$

Substituting with (15),

$$\forall i \in \{1, \dots, \text{left} - 1\} \bullet A[i] = A[n - i + 1])$$

The conjunction of this and (18) is what was to be proved. \square

We have now proved all the assertions we attached to the algorithm. In particular, the correctness assertions for the entire algorithm are the assertion at line 3 and the universal statement that is one conjunct of the assertion at line 8.

2. The following algorithm copies all non-negative elements in array A of integers into array B, which it returns. For example, if A is [3,-1,4,0,-1,5], then [3,4,0,5] is returned. Prove the correctness of this algorithm using the method of loop invariants and well-founded sets. Be sure to attach the appropriate assertions.

```

NON-NEG-COPY(A)
1  i ← 1
2  j ← 0
3  while i ≤ LENGTH[A]
4      do if A[i] ≥ 0
5          then j ← j + 1
6              B[j] ← A[i]
7          i ← i + 1
8  return B

```

Answer

The following is the above algorithm with assertions required by the method of loop invariants added. We again use n as shorthand for $\text{LENGTH}[A]$.

```

NON-NEG-COPY(A)
1  i ← 1
2  j ← 0
3  while i ≤ LENGTH[A] ▶  $i \leq n+1$  and
       $\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y]$ 
4      do if A[i] ≥ 0
5          then j ← j + 1
6              B[j] ← A[i]
7          i ← i + 1
8  return B ▶  $\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, n\} \bullet B[x] = A[y]$ 

```

Here

- B is $i \leq n$,
- INV is $i \leq n+1$ and $\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y]$,
- Q is $\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, n\} \bullet B[x] = A[y]$, and
- S is the loop body.

We first show that $\neg B \wedge \text{INV} \Rightarrow Q$.

So assume $\neg B \wedge \text{INV}$, i.e., assume

$$\neg(i \leq n) \text{ and } i \leq n+1 \text{ and } \forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y]$$

(and show that $\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, n\} \bullet B[x] = A[y]$).

There are three conjuncts here, the first logically equivalent to

$$i > n \quad (1)$$

The other two are

$$i \leq n+1 \quad (2)$$

$$\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y] \quad (3)$$

From (1) and (2),

$$i = n + 1$$

Using this to substitute into (3) gives Q. Q.E.D.

We next show that INV is true when execution first reaches line 3. We assume that A is non-empty, i.e., that $n \geq 1$ (even though this assumption is actually unnecessary). By line 1, $i = 1$, thus $i \leq n$, and so $i \leq n+1$, establishing the first conjunct of INV. By line 2,

$$j = 0 \quad (4)$$

Trivially,

$$\forall x \in \emptyset \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y] \quad (5)$$

By (4),

$$\{1, \dots, j\} = \{1, \dots, 0\} = \emptyset$$

Substituting into (5),

$$\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y],$$

which is the second conjunct of INV. \square

We next show that $B \wedge \text{INV} \{S\} \text{INV}$, i.e., that
if

$$i \leq n \text{ and } i \leq n+1 \text{ and } \forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y]$$

then, after S is executed,

$$\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y]$$

Since $i \leq n$ and $i \leq n+1$ is logically equivalent to $i \leq n$, we assume two things:

$$i \leq n \quad (5)$$

$$\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y] \quad (6)$$

Now, the only change S makes to i is to increment it (line 7). Thus, by (5), after S is executed,

$$i \leq n+1,$$

which is one conjunct of INV.

To establish the second conjunct of INV, we distinguish two cases, depending on whether the at line 4 is true or false.

Case $A[i] \geq 0$ is false:

Then S does not change j but it does increment i (line 7). Fix x at some arbitrary element of $\{1, \dots, j\}$. Assumption (6) guarantees that

$$B[x] \geq 0 \quad (7)$$

Where i' is the value of i before S is executed, we have

$$i = i' + 1$$

or

$$i' = i - 1 \quad (8)$$

Assumption (6) also guarantees that

$$\exists y \in \{1, \dots, i'-1\} \bullet B[x] = A[y]$$

Substituting with (8),

$$\exists y \in \{1, \dots, i-2\} \bullet B[x] = A[y]$$

Now, if there is some $y \in \{1, \dots, i-2\}$ such that $B[x] = A[y]$, then there is a $y \in \{1, \dots, i-1\}$ such that $B[x] = A[y]$. (Just take the same element of A.) Thus,

$$\exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y]$$

Conjoining this with (7),

$$B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y]$$

Since x is an arbitrary element of $\{1, \dots, j\}$, we may generalize:

$$\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y],$$

which is the second conjunct of INV we set out to prove.

Case $A[i] \geq 0$ is true:

Then S increments both i (line 7) and j (line 5). Where i' and j' are the old values of i and j (respectively), we have

$$i = i' + 1$$

or

$$i' = i - 1 \quad (9)$$

and

$$j = j' + 1$$

or

$$j' = j - 1 \quad (10)$$

Assumption (6) in the current notation is

$$\forall x \in \{1, \dots, j'\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i'-1\} \bullet B[x] = A[y]$$

Substituting with (9) and (10),

$$\forall x \in \{1, \dots, j-1\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-2\} \bullet B[x] = A[y] \quad (11)$$

Fix x at some arbitrary element of $\{1, \dots, j\}$. If $x \in \{1, \dots, j-1\}$, then (11) guarantees that $B[x] \geq 0$. If $x = j$, then, by the case assumption and line 6, $B[x] \geq 0$. In any case,

$$B[x] \geq 0 \quad (12)$$

Again, if $x \in \{1, \dots, j-1\}$, then (11) guarantees that

$$\exists y \in \{1, \dots, i-2\} \bullet B[x] = A[y]$$

Since $y \in \{1, \dots, i-2\}$ implies $y \in \{1, \dots, i-1\}$, it follows that

$$\exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y] \quad (13)$$

If, on the other hand, $x = j$, then by line 6,

$$B[x] = A[i']$$

Substituting with (9),

$$B[x] = A[i-1] \tag{14}$$

From (13) (for $x \in \{1, \dots, j-1\}$) and (14) (for $x = j$), it follows that (13) holds for our arbitrary $x \in \{1, \dots, j\}$. Conjoining (12) and (13),

$$B[x] \geq 0 \wedge \exists y \in \{1, \dots, i'-1\} \bullet B[x] = A[y]$$

Since x is an arbitrary element in $\{1, \dots, i'-1\}$, we may generalize:

$$\forall x \in \{1, \dots, j\} \bullet B[x] \geq 0 \wedge \exists y \in \{1, \dots, i-1\} \bullet B[x] = A[y],$$

which again is the second conjunct of INV we set out to prove.

Thus, in either case the second conjunct of INV holds. We have now proved both conjuncts. \square

It remains to show termination using the method of well-founded sets. We must find an expression, in terms of the program variables, that

1. takes on values from an ordered set T such that any decreasing sequence of elements from T reaches a smallest element in a finite number of steps (i.e., T is *well-founded*) and
2. decreases in value on each iteration

An expression that will work is $n-i$. It starts (when loop is first encountered, with $i = 1$) at $n-1$. From the above proof of weak correctness (see the first conjunct in INV and the negation of B), we know that final value of i is $n+1$, so the final value of $n-i$ is -1 . Thus, T is $\{-1, 0, \dots, n-1\}$. Since $n-2$ is finite, T indeed has the property

1. Any decreasing sequence of elements from it reaches a smallest element in a finite number of steps

Also, n is unchanged by the loop and i is changed only at line 7, where it is incremented, so we have the second property, viz.,

2. $n-i$ decreases (by 1) in value on each iteration

Therefore, our loop terminates. \square