CSU44004-Formal Verification Assignment 2
Leong Kai Ler
15334636
November 20, 2019

Question 1

a) $\forall x(0 \leq x < |s| \Rightarrow \exists y \exists z(0 \leq y < z < |s'| \wedge s[x] = s'[y] \wedge s[x] = s'[z] \wedge y \neq z))$

b) $\forall w(0 \leq w < |s| \Rightarrow !(\exists x \exists y \exists z(0 \leq x < y < z < |s'| \wedge s[w] = s'[x] \wedge s[w] = s'[y] \wedge s[w] = s'[z] \wedge x \neq y \wedge y \neq z \wedge x \neq z)))$

c) $\forall x(0 \leq x < |s| \Rightarrow \exists y \exists z(0 \leq y < z < |s'| \wedge s[x] = s'[y] \wedge s[x] = s'[z] \wedge y \neq z \wedge \forall w(0 \leq w < |s'| \wedge y \neq w \wedge z \neq w \Rightarrow s[x] \neq s'[w])))$

d) let a be the integer.
$\forall x(\neg \exists y(0 \leq y < |s| \wedge s[y] = x) \Rightarrow \neg \exists z(0 \leq z < |s'| \wedge s'[z] = x))$

Question 2

Solution 2(a)

$0 \leq lo < |s| \wedge \forall x(0 \leq x < |s| \Rightarrow s[lo] \geq s[x])$

Solution 2(b)

Show $\vdash_{par}$ $(\!|\ 0 < |s|\ |\!)$ findMax $(\!|$T$|\!)$.

Invariant = T
Variant = hi - lo

$(\!|\ 0 < |s|\ |\!)$
$(\!|\ T \wedge 0 < |s|\ |\!)$ ***imp***
lo := 0;
$(\!|\ T \wedge lo < |s|\ |\!)$ ***asg***
$(\!|\ T \wedge lo \leq |s| - 1\ |\!)$ ***imp***
hi := $|s|$ **- 1 ;**
$(\!|\ T \wedge hi < |s|\ |\!)$ ***asg***
$(\!|\ T \wedge hi - lo \geq 0\ |\!)$ ***imp***
while (lo $<$ **hi)** $\{$
    $(\!|\ T \wedge 0 \leq hi - lo = E_o \wedge lo < hi\ |\!)$ ***while***
    $(\!|\ 0 < hi - lo = E_o\ |\!)$ ***imp***
    if $(s[lo] \leq s[hi])$ **then** $\{$
        $(\!|\ 0 < hi - lo = E_o \wedge s[lo] \leq s[hi]\ |\!)$ ***if-statement***
        $(\!|\ 0 \leq hi - (lo + 1) < E_o\ |\!)$ ***imp***
        lo := lo + 1;
        $(\!|\ 0 \leq hi - lo < E_o\ |\!)$ ***asg***
    $\}$
    else $\{$
        $(\!|\ 0 < hi - lo = E_o \wedge \neg(s[lo] \leq s[hi])\ |\!)$ ***if-statement***
        $(\!|\ 0 \leq (hi - 1) - lo < E_o\ |\!)$ ***imp***
        hi := hi - 1 ;
        $(\!|\ 0 \leq hi - lo < E_o\ |\!)$ ***asg***
    $\}$
    $(\!|\ 0 \leq hi - lo < E_o\ |\!)$ ***if-statement***
    $(\!|\ T \wedge 0 \leq hi - lo < E_o\ |\!)$ ***imp***
$\}$
$(\!|\ T \wedge \neg(lo < hi)\ |\!)$ ***while***
$(\!|\ T\ |\!)$

Solution 2(c)

Show $\vdash_{par}$ $(\!|\ 0 < |s|\ |\!)$ findMax $(\!|$ isMax(s, lo)$|\!)$.

Invariant = $isMax(s[..lo+1] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi..], lo+1)$
Variant = hi - lo

$(\!|\ 0 < |s|\ |\!)$
$(\!|\ 0 < |s| \wedge (isMax(s[..0+1] + s[|s|-1..], 0) \vee isMax(s[..0+1] + s[|s|-1..], |s|-1))\ |\!)$ ***imp***
lo := 0;
$(\!|\ lo < |s| \wedge (isMax(s[..lo+1] + s[|s|-1..], lo) \vee isMax(s[..lo+1] + s[|s|-1..], |s|-1))\ |\!)$ ***asg***
hi := $|s|$ **- 1 ;**
$(\!|\ lo \leq hi < |s| \wedge (isMax(s[..lo+1] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi..], lo+1))\ |\!)$ ***asg***
while (lo $<$ **hi)** $\{$
    $(\!|\ lo \leq hi \wedge (isMax(s[..lo+1] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi..], lo+1))\ |\!)$ ***while***
    $(\!|\ (isMax(s[..lo+1] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi..], lo+1))\ |\!)$ ***imp***
    if $(s[lo] \leq s[hi])$ **then** $\{$
        $(\!|\ (isMax(s[..lo+1] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi..], lo+1)) \wedge s[lo] \leq s[hi]\ |\!)$
        if-statement
        $(\!|\ isMax(s[..lo+1] + s[hi..], lo+1)\ |\!)$ ***imp***
        lo := lo + 1;
        $(\!|\ isMax(s[..lo] + s[hi..], lo)\ |\!)$ ***asg***
    $\}$
    else $\{$
        $(\!|\ (isMax(s[..lo+1] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi], lo+1)) \wedge \neg(s[lo] \leq s[hi])\ |\!)$
        if-statement
        $(\!|\ isMax(s[..lo+1] + s[hi..], lo)\ |\!)$ ***imp***
        hi := hi - 1 ;
        $(\!|\ isMax(s[..lo+1] + s[hi+1..], lo)\ |\!)$ ***asg***
    $\}$
    $isMax(s[..lo] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi+1..], lo)$ ***if-statement***
    $lo \leq hi \wedge isMax(s[..lo] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi+1..], lo)$ ***imp***
$\}$
$(\!|\ (isMax(s[..lo] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi+1..], lo)) \wedge \neg(lo < hi)\ |\!)$ ***while***
$(\!|\ (isMax(s[..lo] + s[hi..], lo) \vee isMax(s[..lo+1] + s[hi+1..], lo)) \wedge lo = hi\ |\!)$ ***imp***
$(\!|\ isMax(s[..lo] + s[lo..], lo)\ |\!)$ ***imp***
$(\!|\ isMax(s, lo)\ |\!)$

Question 3

Solution 3(a)

$\forall x(0 \leq x < \frac{|s|}{2} \Rightarrow s[x] = s[|s| - x - 1])$

Solution 3(b)

Show $\vdash_{tot}$ $(\!|\ 0 \leq |s|\ |\!)$ checkPalindrome $(\!|\ T\ |\!)$.

Invariant = T
Variant = j - i

$(\!|\ 0 \leq |s|\ |\!)$
$(\!|\ T \wedge 0 \leq |s|\ |\!)$ ***imp***
res := 1;
var i := 0;
$(\!|\ T \wedge i \leq |s|\ |\!)$ ***asg***
$(\!|\ T \wedge i - 1 \leq |s| - 1\ |\!)$ ***imp***
var j := $|s|$ **- 1;**
$(\!|\ T \wedge -1 \leq j\ |\!)$ ***asg***
$(\!|\ T \wedge i - 1 \leq j\ |\!)$ ***imp***
$(\!|\ T \wedge -1 \leq j - i\ |\!)$ ***imp***
$(\!|\ T \wedge j - i + 1 \geq 0\ |\!)$ ***imp***
while (i $<$ **j** $\&$ **res = 1)**
$\{$
$(\!|\ T \wedge i < j \wedge res = 1 \wedge 0 \leq j - i + 1 = E_o\ |\!)$ ***while***
$(\!|\ T \wedge j - i > 0 \wedge res = 1 \wedge 0 \leq j - i + 1 = E_o\ |\!)$ ***imp***
$(\!|\ T \wedge res = 1 \wedge 0 < j - i < E_o\ |\!)$ ***imp***
if (s[i] != s[j])
$\{$
$(\!|\ i < j \wedge res = 1 \wedge 0 \leq j - i + 1 = E_o \wedge s[i]! = s[j]\ |\!)$ ***if-statement***
res := 0
$(\!|\ 0 \leq j - i + 1 < E_o\ |\!)$ ***imp***
$\}$
else
$\{$
$(\!|\ i < j \wedge res = 1 \wedge 0 \leq j - i + 1 = E_o \wedge \neg(s[i]! = s[j])\ |\!)$ ***if-statement***
skip
$(\!|\ 0 \leq j - i + 1 < E_o\ |\!)$ ***imp***
$\}$
$(\!|\ T \wedge 0 \leq (j - 1) - (i + 1) + 1 < E_o\ |\!)$ ***imp***
i := i + 1;
$(\!|\ T \wedge 0 \leq (j - 1) - i + 1 < E_o\ |\!)$ ***asg***
j := j - 1;
$(\!|\ T \wedge 0 \leq j - i + 1 < E_o\ |\!)$ ***asg***
$\}$
$(\!|\ T \wedge (j <= i\ ||\ res = 0)\ |\!)$ ***while***
$(\!|\ T\ |\!)$

Solution 3(c)

Show $\vdash_{par}$ $(\!|\ 0 \leq |s|\ |\!)$ checkPalindrome $(\!|\ (res == 1) \Leftrightarrow$ isPal(s)$|\!)$.

Invariant = $res = 1 \Leftrightarrow isPal(s[..i] + s[j+1..]$
Variant = j - i + 1

Let
$I_2 = 0 \leq i < j + 1 \leq |s|$

$(\!|\ 0 \leq |s|\ |\!)$
$(\!|\ I_2 \wedge 1 = 1 \Rightarrow isPal(s[..0] + s[0-1+1..]) \wedge isPal(s[..0] + s[0-1+1..]) \Rightarrow 1 = 1\ |\!)$ ***imp***
res := 1;
var i := 0;
var j := $|s|$ - 1;
$(\!|\ I_2 \wedge res = 1 \Rightarrow isPal(s[..0] + s[0-1+1..]) \wedge isPal(s[..0] + s[0-1+1..]) \Rightarrow res = 1\ |\!)$ ***asg***
while (i $<$ j $\&$ res = 1)
{
$(\!|\ I_2 \wedge \text{res} == 1 \Rightarrow isPal(s[..i] + s[j+1..]) \wedge isPal(s[..i] + s[j+1..]) \Rightarrow \text{res} == 1\ |\!)$ ***while***
$(\!|\ I_2 = \wedge\ (s[i]! = s[j] \Rightarrow (0 \neq 1 \wedge isPal(s[..i] + s[j+1..]))) \wedge \neg(s[i]! = s[j] \Rightarrow (1 \neq 1 \wedge isPal(s[..i] + s[j+1..])))\ |\!)$ ***if-statement***
if (s[i] != s[j])
{
$(\!|\ 0 \neq 1 \wedge isPal(s[..i] + s[j+1..])\ |\!)$***imp***
res := 0
$(\!|\ res == 0 \wedge isPal(s[..i+1] + s[j..])\ |\!)$***imp***
$(\!|$ res $== 1 \Rightarrow isPal(s[..i+1] + s[j..]) \wedge isPal(s[..i+1] + s[j..]) \Rightarrow$ res $== 1$***imp***
}
}
else
{
$(\!|\ 1 == 1 \wedge isPal(s[..i] + s[j+1..])\ |\!)$***imp***
skip
$(\!|\ res == 1 \wedge isPal(s[..i+1] + s[j..])\ |\!)$***imp***
$(\!|$ res $== 1 \Rightarrow isPal(s[..i+1] + s[j..]) \wedge isPal(s[..i+1] + s[j..]) \Rightarrow$ res $== 1$***imp***
}
$(\!|\ I_2 \wedge$ res $== 1 \Rightarrow isPal(s[..i+1] + s[j..]) \wedge isPal(s[..i+1] + s[j..]) \Rightarrow$ res $== 1$***if-statement***
$(\!|\ I_2 \wedge$ res $== 1 \Rightarrow isPal(s[..i+1] + s[j+1-1..]) \wedge isPal(s[..i+1] + s[j+1-1..]) \Rightarrow$ res $== 1\ |\!)$ ***imp***
i := i + 1;
$(\!|\ I_2 \wedge$ res $== 1 \Rightarrow isPal(s[..i] + s[j+1-1..]) \wedge isPal(s[..i+1] + s[j+1-1..]) \Rightarrow$ res $== 1\ |\!)$ ***asg***
j := j - 1;
$(\!|\ I_2 \wedge$ res $== 1 \Rightarrow isPal(s[..i] + s[j+1..]) \wedge isPal(s[..i] + s[j+1..]) \Rightarrow$ res $== 1\ |\!)$ ***asg***
}
$(\!|\ I_2 \wedge$ res $== 1 \Rightarrow isPal(s[..i] + s[j+1..]) \wedge isPal(s[..i] + s[j+1..]) \Rightarrow$ res $== 1 \wedge \neg(i < j \wedge res = 1)\ |\!)$ ***while***
$(\!|\ I_2 \wedge$ res $== 1 \Rightarrow isPal(s[..i] + s[j+1..]) \wedge isPal(s[..i] + s[j+1..]) \Rightarrow$ res $== 1 \wedge i = j\ |\!)$ ***imp***
$(\!|$ res $== 1 \Rightarrow isPal(s) \wedge isPal(s) \Rightarrow$ res $== 1\ |\!)$ ***imp***

$(\!|\ \text{res} == 1 \Leftrightarrow \text{isPal(s)}\ |\!)$

Question 4

Solution 4(a)

Show $\vdash_{tot}$ $(\!|\ 0 < |s|\ |\!)$ findMax $(\!|$ isMax(s, lo)$|\!)$.

```
method findMax(s: seq<int>) returns(lo: int)
requires |s| > 0
ensures isMax(s, lo)
{
    assert(|s| > 0);
    assert(0 < 1 <= |s| && isMax(s[..1], 0));
    lo := 0;
    assert(0 <= lo < |s| && isMax(s[..1], lo));
    var hi : int := |s| - 1 ;
    assert(0 <= hi < |s| && isMax(s[hi..], 0));
    assert(hi - lo >= 0);
    while (lo < hi)
        decreases hi - lo
        invariant 0 <= lo <= hi < |s|
        invariant (isMax2(s, 0, lo, lo) && isMax2(s, hi, |s|-1 , lo)) || (
           isMax2(s, 0, lo, hi) && isMax2(s, hi, |s|-1 , hi))
    {
        if(s[lo] <= s[hi])
        {
            lo := lo + 1;
        }
        else
        {
            hi := hi - 1;
        }
    }
}

predicate isMax2(s: seq<int>, lo: int, hi: int, max: int){
    0 <= max < |s| && 0 <= lo <= hi < |s| && forall x : int :: lo <= x <= hi
       ==> s[max] >= s[x]
}

predicate isMax(s : seq<int>, lo: int){
    0 <= lo < |s| && forall x: int :: 0 <= x < |s| ==> s[lo] >= s[x]
}
```

Solution 4(b)

Show $\vdash_{par}$ $(\!|\ T\ |\!)$ checkPalindrome $(\!|\ (res == 1) \Leftrightarrow \text{isPal(s)}|\!)$.

```
method checkPalindrome(s: seq<int>) returns (res: bool)
requires |s| >= 0
ensures isPalindrome(s) <==> res == true
{
    res := true;
    var i := 0 ;
    var j := | s | - 1 ;
    while ( i < j && res == true)
    invariant i == |s| -1 - j && i <= |s| && ((forall k :: 0 <= k < i ==> s[k]
        == s[|s|-k-1]) <==> res == true)
    decreases |s| - i
    {
        if (s[i] != s[j])
        {
            res := false;
        }
        else {

        }
        i := i + 1 ;
        j := j - 1;
    }
}

predicate palindrome(s1: seq<int>, s2: seq<int>)
{
    |s1| == |s2| && forall x : int :: 0 <= x < |s1| ==> s1[x] == s2[|s2|-x-1]
}

predicate isPalindrome(s: seq<int>)
{
    forall x : int :: 0 <= x < |s| ==> s[x] == s[|s|-x-1]
}
```