Assignment 1

z5141448 Ruofei HUANG

April 6, 2018

Defanations

Two Dimensional Arrays Expression

To describe variants of two-dimensional arrays we write $(b : k \mapsto j \mapsto x)$ instead of $(b : k \mapsto (b[k] : j \mapsto x))$. We use this new notation to state an instance of the array-assignment axiom we saw already

$$\left\{\phi[^{(b:k\mapsto x)}/_b]\right\} b[k] := x \left\{\phi\right\}$$

for two-dimensional arrays:

$$\left\{\phi[^{(b:k\mapsto j\mapsto x)}/_b]\right\} b[k][j] := x \left\{\phi\right\}$$

String Length

A string $S \in \mathit{Letter}^*$ which is an array of letters[1].Also, string will be terminate by the null character which is a convention by the C programming language and we will follow this convention in this proof. We write $|S|$ for the number of letters in the string. Formally, we define these two nothion inductively by

$$|S\ell| = |S| + \begin{cases} 1 & \text{if } \ell \neq' \backslash 0' \\ 0 & \text{if } \ell =' \backslash 0' \end{cases}$$

Also, by the convention of C we has this definition for $S \in \mathit{string}$.

$$S[|S|] =' \backslash 0' \wedge \forall 0 \leq i < |S| \, (S[i] \neq' \backslash 0')$$

[1]The letter here is a legal charater encode with ASCII, UTF-8 or other charater encoding standard.

String Equals

To describe two string a, b $(a, b \in String)$ are equals we write $a = b$ when:

$$a = b \iff |a| = |b| \wedge \forall j \in 0..|a|\,(a[j] = b[j])$$

Similarly, we write:

$$a \neq b \iff \neg(a = b)$$

Comparing String

After defining what is string equal, we need a pieces programme in toy language to do the dirty work which could compare two strings.

String Assign

To assign a string to another string array, we will denote as

$$a := b$$

instead of a long programme of our toy language:

$\{a, b \in String\}$
$\{I[^0/_i]\}$
$i := 0;$
$\{I\}$
while $i \leq |b|$ **do**
  $\{I \wedge i \leq |b|\}$
  $\{I[^{i+1}/_i][^{a:i \mapsto b[i]}/_a]\}$
  $a[i] := b[i];$
  $\{I[^{i+1}/_i]\}$
  $i := i + 1;$
  $\{I\}$
od;
$\{I \wedge i > |b|\}$
$\{a, b \in String \wedge a = b\}$

when our invariant is

$$I = a, b \in String \wedge 0 \leq i \leq (|b| + 1) \wedge \forall k \in 0..(i - 1)\,(a[k] = b[k])$$

Here are the proofs of the implications:

First Implication for String assign: $a, b \in String \Rightarrow I[^0/_i]$

$$
\begin{array}{ll}
& a, b \in String \\
\Rightarrow & \quad \langle \text{using } |b| \in \mathbb{N} \text{ and realising that the last conjunct is vacuously true} \rangle \\
& a, b \in String \land 0 \leq 0 \leq (|b| + 1) \land \forall k \in 0..(0 - 1)\,(a[k] = b[k]) \\
\Leftrightarrow & \quad \langle \text{definition of I and substitution} \rangle \\
& I[^0/_i]
\end{array}
$$

Second Implication $I \land i \leq |b| \Rightarrow I[^{i+1}/_i][^{a:i \mapsto b[i]}/_a]$

We first look at the LHS:

$$
\begin{array}{ll}
& I \land i \leq |b| \\
\Leftrightarrow & \quad \langle \text{Substitue I } \rangle \\
& a, b \in String \land 0 \leq i \leq (|b| + 1) \land \forall k \in 0..(i - 1)\,(a[k] = b[k]) \land i \leq |b| \\
\Leftrightarrow & \quad \langle \text{Conjunct } i \leq (|b| + 1) \text{ and } i \leq |b| \rangle \\
& a, b \in String \land 0 \leq i \leq |b| \land \forall k \in 0..(i - 1)\,(a[k] = b[k])
\end{array}
$$

We then expand RHS:

$$
\begin{array}{ll}
& I[^{i+1}/_i][^{a:i \mapsto b[i]}/_a] \\
\Leftrightarrow & \quad \langle \text{substitute } i = i + 1 \text{ and } a[i] = b[i] \text{ by definition} \rangle \\
& a, b \in String \land 0 \leq i + 1 \leq (|b| + 1) \land \forall k \in 0..((i + 1) - 1)\,(a[k] = b[k]) \land a[i] := b[i]
\end{array}
$$

We then have a clear imply

$$
\begin{array}{ll}
& a, b \in String \land 0 \leq i \leq |b| \land \forall k \in 0..(i - 1)\,(a[k] = b[k]) \\
\Rightarrow & \quad \langle i \leq |b| \Rightarrow i + 1 \leq |b| + 1 \text{ and } a[i] := b[i] \rangle \\
& a, b \in String \land 0 \leq i + 1 \leq (|b| + 1) \land \forall k \in 0..((i + 1) - 1)\,(a[k] = b[k]) \land a[i] := b[i]
\end{array}
$$

Third Implication $I \land i > |b| \Rightarrow a, b \in String \land a = b$

$$
\begin{array}{ll}
& I \land i > |b| \\
\Leftrightarrow & \quad \langle \text{substitution of I } \rangle \\
& a, b \in String \land 0 \leq i \leq (|b| + 1) \land \forall k \in 0..(i - 1)\,(a[k] := b[k]) \land i > |b| \\
\Leftrightarrow & \quad \langle\ i > |b| \text{and } i \leq (|b| + 1) \text{ with some calculation} \rangle \\
& a, b \in String \land \forall k \in 0..\,|b|\,(a[k] := b[k]) \\
\Rightarrow & \quad \langle \text{Definition of two string equal} \rangle \\
& a, b \in String \land a = b
\end{array}
$$

1 Task 1

Since we have define some manipulation of String, we can see a string as a whole. So the input is an array of String. Also , the ouput is store in b which is an empty array (type is $String*$ too). Hence we can define our precondiction as:

$$a, b \in String^* \wedge |a| = n$$

As the post condition as:

$$\forall i < n \, (a[i] = b[m(a, i)])$$

Where m is a mapping function define recursively as follow:

$$m(a,i) = \begin{cases} 0 & \text{if } i = 0 \\ m(i-1) & \text{if } a[i] = a[i-1] \\ m(i-1)+1 & \text{if } a[i] \neq a[i-1] \end{cases}$$

2 Task 2

We propose the following proof outline to demonstrate the correctness of our code (in black).

$\{a, b \in String^* \wedge |a| = n\}$ (1)
$\{J\}$ (2)
if $|a| > 0$ **then** (3)
  $\{J \wedge |a| > 0\}$ (4)
  $\{I[^1/_j][^1/_i][^{b:0 \mapsto a[0]}/_b]\}$ (5)
  $b[0] := a[0];$ (6)
  $\{I[^1/_j][^1/_i]\}$ (7)
  $i = 1; j = 1;$ (8)
  $\{I\}$ (9)
else (10)
  $\{J \wedge |a| \leq 0\}$ (11)
  $\{I[^0/_i][^0/_j]\}$ (12)
  $i := 0; j := 0;$ (13)
  $\{I\}$ (14)
fi (15)
$\{I\}$ (16)
while $i < |a|$ **do** (17)
  $\{I \wedge i < |a|\}$ (18)
  $\{K\}$ (19)
  if $a[i] \neq a[i-1]$ **then** (20)
    $\{K \wedge a[i] \neq a[i-1]\}$ (21)
    $\{I[^{i+1}/_i][^{j+1}/_j][^{b:j \mapsto a[i]}/_b]\}$ (22)
    $b[j] := a[i];$ (23)
    $\{I[^{i+1}/_i][^{j+1}/_j]\}$ (24)
    $j := j + 1;$ (25)
    $\{I[^{i+1}/_i]\}$ (26)
  else (27)
    $skip$ (28)
  fi (29)
  $\{I[^{i+1}/_i]\}$ (30)
  $i := i + 1$ (31)
  $\{I\}$ (32)
od (33)
$\{I \wedge i \geq |a|\}$ (34)
$\{\forall i < n\,(a[i] = b[m(a, i)])\}$ (35)

Here are the invariants of this programme [2]:

$$I = a, b \in String^* \wedge |a| = n \wedge 0 \leq i \leq |a| \wedge \forall k \in 0..(i-1)\,(a[k] = b[m(a,k)])$$
$$J = \begin{pmatrix} |a| > 0 \Rightarrow I[^1/_j][^1/_i][^{b:0 \mapsto a[0]}/_b] \\ |a| \leq 0 \Rightarrow I[^0/_j][^0/_i] \end{pmatrix}$$
$$K = \begin{pmatrix} a[i] \neq a[i-1] \Rightarrow I[^{i+1}/_i][^{j+1}/_j][^{b:j \mapsto a[i]}/_b] \\ a[i] = a[i-1] \Rightarrow I[^{i+1}/_i] \end{pmatrix}$$

2.1 First Implication: $a, b \in String^* \wedge |a| = n \Rightarrow J$

$$\begin{array}{ll} & a, b \in String^* \wedge |a| = n \\ \Rightarrow & \quad \langle n \in \mathbb{N}, \text{substitution of } i, j \rangle \\ & \begin{pmatrix} |a| > 0 \Rightarrow a, b \in String^* \wedge |a| = n \wedge 0 \leq 1 \leq |a| \wedge \forall k \in 0..(1-1)\,(a[k] = b[m(a,k)]) \\ |a| = 0 \Rightarrow a, b \in String^* \wedge |a| = n \wedge 0 \leq 0 \leq |a| \wedge \forall k \in 0..(0-1)\,(a[k] = b[m(a,k)]) \end{pmatrix} \\ \Rightarrow & \quad \langle \text{Substitution of I} \rangle \\ & \begin{pmatrix} |a| > 0 \Rightarrow I[^1/_j][^1/_i][^{b:0 \mapsto a[0]}/_b] \\ |a| \leq 0 \Rightarrow I[^0/_j][^0/_i] \end{pmatrix} \\ \Leftrightarrow & \quad \langle \text{Definition of J} \rangle \\ & J \end{array}$$

[2] The invariant is following the case study in week 8, might not be true for the stuff we study for now. But I have to use this tool otherwise I couldn't countinue this proof

2.2 Second Implication: $I \wedge i < |a| \Rightarrow K$

$$
\begin{array}{ll}
& I \wedge i < |a| \\
\Leftrightarrow & \quad \langle \text{Definition of } I \rangle \\
& a, b \in String^* \wedge |a| = n \wedge 0 \leq i \leq |a| \wedge \forall k \in 0..(i-1)\,(a[k] = b[m(a,k)]) \wedge i < |a| \\
\Rightarrow & \quad \langle \text{Substitue } i+1 \text{ and } j+1 \text{ and } K \rangle \\
& \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\ 0 \leq i+1 \leq |a|+1 \wedge \forall k \in 0..(i)\,(a[k] = b[m(a,k)]) \wedge i < |a| \\ a[i] = a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\ 0 \leq i+1 \leq |a|+1 \wedge \forall k \in 0..(i)\,(a[k] = b[m(a,k)]) \wedge i < |a| \end{array} \right) \\
\Rightarrow & \quad \langle \text{Conjunct the } i < |a| \rangle \\
& \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\ 0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i)\,(a[k] = b[m(a,k)]) \\ a[i] = a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\ 0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i)\,(a[k] = b[m(a,k)]) \end{array} \right) \\
\Leftrightarrow & \quad \langle \rangle \\
& \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow I[^{i+1}/_i][^{j+1}/_j][^{b:j \mapsto a[i]}/_b] \\ a[i] = a[i-1] \Rightarrow I[^{i+1}/_i] \end{array} \right) \\
\Leftrightarrow & \quad \langle \rangle \\
& \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow I[^{i+1}/_i][^{j+1}/_j][^{b:j \mapsto a[i]}/_b] \\ a[i] = a[i-1] \Rightarrow I[^{i+1}/_i] \end{array} \right) \\
\Leftrightarrow & \quad \langle \text{Definition of K} \rangle \\
& K
\end{array}
$$

3 Task 3

4 Task 4