Assignment 1

z5141448 Ruofei HUANG

April 8, 2018

Definations

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 $S \in \mathit{string}$.

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

[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 $(a, b \in \mathit{String})$ are equals we write $a = b$ when:

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

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:

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

when our invariant is

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

Here are the proofs of the implications:

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

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

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

We first look at the LHS:

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

We then expand RHS:

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

We then have a clear imply

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

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

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

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).

$$\{a, b \in \mathit{String}^* \wedge |a| = n\} \tag{1}$$

$$\{J\} \tag{2}$$

$$\textbf{if } |a| > 0 \textbf{ then} \tag{3}$$

$$\quad \{J \wedge |a| > 0\} \tag{4}$$

$$\quad \{I[{}^{1}/_{j}][{}^{1}/_{i}][{}^{b:0\mapsto a[0]}/_{b}]\} \tag{5}$$

$$\quad b[0] := a[0]; \tag{6}$$

$$\quad \{I[{}^{1}/_{j}][{}^{1}/_{i}]\} \tag{7}$$

$$\quad i = 1; j = 1; \tag{8}$$

$$\quad \{I\} \tag{9}$$

$$\textbf{else} \tag{10}$$

$$\quad \{J \wedge |a| \leq 0\} \tag{11}$$

$$\quad \{I[{}^{0}/_{i}][{}^{0}/_{j}]\} \tag{12}$$

$$\quad i := 0; j := 0; \tag{13}$$

$$\quad \{I\} \tag{14}$$

$$\textbf{fi} \tag{15}$$

$$\{I\} \tag{16}$$

$$\textbf{while } i < |a| \textbf{ do} \tag{17}$$

$$\quad \{I \wedge i < |a|\} \tag{18}$$

$$\quad \{K\} \tag{19}$$

$$\quad \textbf{if } a[i] \neq a[i-1] \textbf{ then} \tag{20}$$

$$\qquad \{K \wedge a[i] \neq a[i-1]\} \tag{21}$$

$$\qquad \{I[{}^{i+1}/_{i}][{}^{j+1}/_{j}][{}^{b:j\mapsto a[i]}/_{b}]\} \tag{22}$$

$$\qquad b[j] := a[i]; \tag{23}$$

$$\qquad \{I[{}^{i+1}/_{i}][{}^{j+1}/_{j}]\} \tag{24}$$

$$\qquad j := j + 1; \tag{25}$$

$$\qquad \{I[{}^{i+1}/_{i}]\} \tag{26}$$

$$\quad \textbf{else} \tag{27}$$

$$\qquad \mathit{skip} \tag{28}$$

$$\quad \textbf{fi} \tag{29}$$

$$\quad \{I[{}^{i+1}/_{i}]\} \tag{30}$$

$$\quad i := i + 1 \tag{31}$$

$$\quad \{I\} \tag{32}$$

$$\textbf{od} \tag{33}$$

$$\{I \wedge i \geq |a|\} \tag{34}$$

$$\{\forall i < n\,(a[i] = b[m(a, i)])\} \tag{35}$$

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

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

$\Rightarrow$ $\langle n \in \mathbb{N}$, substitution of i, j $\rangle$

$$\begin{pmatrix} |a| > 0 \Rightarrow a, b \in String^* \wedge |a| = n \wedge 0 \leq 1 \leq |a| \wedge \forall k \in 0..(1-1)\,(a[k] = b[m(a,k)]) \\ |a| = 0 \Rightarrow a, b \in String^* \wedge |a| = n \wedge 0 \leq 0 \leq |a| \wedge \forall k \in 0..(0-1)\,(a[k] = b[m(a,k)]) \end{pmatrix}$$

$\Rightarrow$ $\langle$Substitution of I $\rangle$

$$\begin{pmatrix} |a| > 0 \Rightarrow I[^1/_j][^1/_i][^{b:0\mapsto a[0]}/_b] \\ |a| \leq 0 \Rightarrow I[^0/_j][^0/_i] \end{pmatrix}$$

$\Leftrightarrow$ $\langle$Definition of J$\rangle$

$$J$$

[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: $I \wedge i < |a| \Rightarrow K$

$$
\begin{aligned}
& I \wedge i < |a| \\
\Leftrightarrow \quad & \langle \text{Definition of } I \rangle \\
& a, b \in String^* \wedge |a| = n \wedge 0 \leq i \leq |a| \wedge \forall k \in 0..(i-1)\,(a[k] = b[m(a,k)]) \wedge i < |a| \\
\Rightarrow \quad & \langle m(a,i) \text{ need to consider two situation of } a[i] \ (a[i] = a[i-1] \text{ and } a[i] \neq a[i-1]) \rangle \\
& \begin{pmatrix}
a[i] \neq a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\
0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i-1)\,(a[k] = b[m(a,k)]) \\
\wedge a[i] = b[j-1] \\
a[i] = a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\
0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i-1)\,(a[k] = b[m(a,k)]) \\
\wedge a[i] = b[j]
\end{pmatrix} \\
\Leftrightarrow \quad & \langle \text{By the recursively definition of } m(a,i) \rangle \\
& \begin{pmatrix}
a[i] \neq a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\
0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i-1)\,(a[k] = b[m(a,k)]) \\
\wedge a[i] = b[m(a,i)] \\
a[i] = a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\
0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i-1)\,(a[k] = b[m(a,k)]) \\
\wedge a[i] = b[m(a,i)]
\end{pmatrix} \\
\Leftrightarrow \quad & \langle \text{Merge two cases of } k \ (k = i \text{ and } k \in 0..(i-1)) \ . \rangle \\
& \begin{pmatrix}
a[i] \neq a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\
0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i)\,(a[k] = b[m(a,k)]) \\
a[i] = a[i-1] \Rightarrow a, b \in String^* \wedge |a| = n \wedge \\
0 \leq i+1 \leq |a| \wedge \forall k \in 0..(i)\,(a[k] = b[m(a,k)])
\end{pmatrix} \\
\Leftrightarrow \quad & \langle \text{Substitue back by definition of I.} \rangle \\
& \begin{pmatrix}
a[i] \neq a[i-1] \Rightarrow I[^{i+1}/_i][^{j+1}/_j][^{b:j \mapsto a[i]}/_b] \\
a[i] = a[i-1] \Rightarrow I[^{i+1}/_i]
\end{pmatrix} \\
\Leftrightarrow \quad & \langle \text{Definition of K} \rangle \\
& K
\end{aligned}
$$

The meaning of "By the recursively definition of $m(a,i)$" is when $a[i] = a[i-1]$, a[i] $=$ $b[m(a,i-1)]$, which $m(a,i-1) = j-1$ since $j = |b|$.

3 Task 3

4 Task 4