

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

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

for two-dimensional arrays:

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

String Length

A string $S \in Letter^*$ which is an array of letters¹. 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 $S \in string$.

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

¹The 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 ∈ String}
{I0/i}
i := 0;
{I}
while i ≤ |b| do
  {I ∧ i ≤ |b|}
  {Ii+1/i}[a:i→b[i]/a]}
  a[i] := b[i];
  {Ii+1/i}
  i := i + 1;
  {I}
od;
{I ∧ i > |b|}
{a, b ∈ String ∧ 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: $a, b \in \text{String} \Rightarrow I[{}^0/i]$

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

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

We first look at the LHS:

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

We then expand RHS:

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

We then have a clear imply

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

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

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

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 precondition as:

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

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).

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

Here are the invariants of this programme ²:

$$\begin{aligned}
I &= a, b \in \text{String}^* \wedge |a| = n \wedge 0 \leq i \leq |a| \wedge \forall k \in 0..(i-1) (a[k] = b[m(a, k)]) \\
J &= \left(\begin{array}{l} |a| > 0 \Rightarrow I[1/j][1/i][b:0 \rightarrow a[0]/b] \\ |a| \leq 0 \Rightarrow I[0/j][0/i] \end{array} \right) \\
K &= \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow I[i+1/i][j+1/j][b:j \rightarrow a[i]/b] \\ a[i] = a[i-1] \Rightarrow I[i+1/i] \end{array} \right)
\end{aligned}$$

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

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

²The 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 continue this proof

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

$$\begin{aligned}
& I \wedge i < |a| \\
\Leftrightarrow & \langle \text{Definition of } I \rangle \\
& a, b \in \text{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 & \langle m(a, i) \text{ need to consider two situation of } a[i] \text{ (} a[i] = a[i-1] \text{ and } a[i] \neq a[i-1]) \rangle \\
& \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow a, b \in \text{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 \text{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{array} \right) \\
\Leftrightarrow & \langle \text{By the recursively definition of } m(a, i) \rangle \\
& \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow a, b \in \text{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 \text{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{array} \right) \\
\Leftrightarrow & \langle \text{Merge two cases of } k \text{ (} k = i \text{ and } k \in 0..(i-1) \text{) .} \rangle \\
& \left(\begin{array}{l} a[i] \neq a[i-1] \Rightarrow a, b \in \text{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 \text{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 & \langle \text{Substitutue back by definition of I.} \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 & \langle \text{Definition of K} \rangle \\
& K
\end{aligned}$$

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

3 Task 3

4 Task 4