COMP2111 Assignment 1

z5160405 Nathan Ellis

April 11, 2018

1 Task 1

We define our precondition (in accordance with the assignment 1 (18s1) specification)

$$n \in \mathbb{N} \wedge a_0 = a \wedge n_0 = n$$

so that it successfully states n is a non-negative integer. We also freeze a's and n's initial value for later reference in the postcondition

$$\alpha \in \mathbb{N} \wedge \forall \alpha < n.\, (a[\alpha] = b[m(\alpha)]) \wedge m(n) = k \wedge a = a_0 \wedge n = n_0$$

which states that the output of our program is stored in array b, with adjacent identical strings collapsed to one upon termination of our program. Also, this postcondition states that the number of strings in b is k. a and n are also assured of remaining unchanged by the program as they retain their initial values.

Clearly, we need to define m regarding the function as seen in the (above) postcondition. So, we do so

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

such that m is an index mapping function describing the adjacent identical strings collapsing as per the program requirements.

2 Task 2

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

$\{n \in \mathbb{N} \wedge a_0 = a \wedge n_0 = n\}$
$\{I[^0/_k][^0/_j][^0/_i]\}$
$i := 0;$
$\{I[^0/_k][^0/_j]\}$
$j := 0;$
$\{I[^0/_k]\}$
$k := 0;$
$\{I\}$
while $i < n$ **do**
    $\{I \wedge 0 \leq i < n\}$
    $\{J[^0/_j]\}$
    $j := 0;$
    $\{J\}$
    while $k \neq 0 \wedge a[i][j] \neq 0 \wedge a[i][j] = b[k-1][j]$ **do**
        $\{J \wedge k \neq 0 \wedge a[i][j] \neq 0 \wedge a[i][j] = b[k-1][j]\}$
        $\{J[^{j+1}/_j]\}$
        $j := j + 1;$
        $\{J\}$
    od;
    $\{I \wedge (k = 0 \vee a[i][j] = 0 \vee a[i][j] \neq b[k-1][j])\}$
    if $k = 0 \vee a[i][j] \neq b[k-1][j]$
        $\{J \wedge (k = 0 \vee a[i][j] = 0 \vee a[i][j] \neq b[k-1][j]) \wedge (k = 0 \vee a[i][j] \neq b[k-1][j])\}$
        $\{K[^0/_j]\}$
        $j := 0;$
        $\{K\}$
        while $a[i][j] \neq 0$ **do**
            $\{K \wedge a[i][j] \neq 0\}$
            $\{K[^{j+1}/_j][^{b:k \mapsto j \mapsto a[i][j]}/_b]\}$
            $b[k][j] := a[i][j];$
            $\{K[^{j+1}/_j]\}$

$j := j + 1;$

$\{K\}$

od;

$\{K \wedge a[i][j] = 0\}$

$\left\{K[^{j+1}/_j][^{b:k \mapsto j \mapsto 0}/_b]\right\}$

$b[k][j] := 0;$

$\left\{K[^{j+1}/_j]\right\}$

$j := j + 1;$

$\{K\}$

$\left\{I[^{i+1}/_i][^{k+1}/_k] \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i] = b[k]\right\}$

$k := k + 1;$

$\left\{I[^{i+1}/_i] \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i] = b[k]\right\}$

else

$\left\{I[^{i+1}/_i] \wedge 0 \leq i < n \wedge k \neq 0 \wedge a[i][j] = b[k-1][j]\right\}$

$skip;$

$\left\{I[^{i+1}/_i] \wedge 0 \leq i < n \wedge k \neq 0 \wedge a[i][j] = b[k-1][j]\right\}$

fi;

$\left\{I[^{i+1}/_i] \wedge 0 \leq i < n\right\}$

$\left\{I[^{i+1}/_i]\right\}$

$i := i + 1;$

$\{I\}$

od;

$\{I \wedge i \geq n\}$

$\{\alpha \in \mathbb{N} \wedge \forall \alpha < n.\, (a[\alpha] = b[m(\alpha)]) \wedge m(n) = k \wedge a = a_0 \wedge n = n_0\}$

where our invariants are

$$\begin{aligned}
I &= \alpha \in \mathbb{N} \wedge \forall \alpha < i.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq i \leq n \wedge m(i) = k \wedge a_0 = a \wedge n_0 = n \\
J &= I \wedge \beta \in \mathbb{N} \wedge \forall \beta < j.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n \\
K &= I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1])
\end{aligned}$$

The only remaining proof obligations are the nine implications between adjacent assertions.

2.1 First implication: $n \in \mathbb{N} \wedge a_0 = a \wedge n_0 = n \Rightarrow I[^0/_k][^0/_j][^0/_i]$

$$
\begin{aligned}
& I[^0/_k][^0/_j][^0/_i] \\
\Leftrightarrow \quad & \langle \text{definition of } I \text{ and substitution} \rangle \\
& \alpha \in \mathbb{N} \wedge \forall \alpha < 0.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq 0 \leq n \wedge m(0) = 0 \wedge a_0 = a \wedge n_0 = n \\
\Leftrightarrow \quad & \langle \text{1st, 2nd and 4th conjuncts are vacuously true and can therefore be discarded} \rangle \\
& 0 \leq 0 \leq n \wedge a_0 = a \wedge n_0 = n \\
\Leftrightarrow \quad & \langle \text{definition of natural numbers} \rangle \\
& n \in \mathbb{N} \wedge a_0 = a \wedge n_0 = n
\end{aligned}
$$

Through logical equivalence, it is obvious that logical implication exists in both directions.

2.2 Second implication: $I \wedge 0 \leq i < n \Rightarrow J[^0/_j]$

$$
\begin{aligned}
& J[^0/_j] \\
\Leftrightarrow \quad & \langle \text{definition of } J \text{ and substitution} \rangle \\
& I \wedge \beta \in \mathbb{N} \wedge \forall \beta < 0.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n \\
\Leftrightarrow \quad & \langle \text{the 2nd conjunct is vacuously true and can therefore be discarded} \rangle \\
& I \wedge 0 \leq i < n
\end{aligned}
$$

Through logical equivalence, it is obvious that logical implication exists in both directions.

2.3 Third implication: $J \wedge k \neq 0 \wedge a[i][j] \neq 0 \wedge a[i][j] = b[k-1][j] \Rightarrow J[^{j+1}/_j]$

$$
\begin{aligned}
& J \wedge k \neq 0 \wedge a[i][j] \neq 0 \wedge a[i][j] = b[k-1][j] \\
\Leftrightarrow \quad & \langle \text{definition of } J \rangle \\
& I \wedge \beta \in \mathbb{N} \wedge \forall \beta < j.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n \wedge k \neq 0 \\
& \wedge a[i][j] \neq 0 \wedge a[i][j] = b[k-1][j] \\
\Leftrightarrow \quad & \langle \text{the last conjunct forms the '}j\text{th' case for the third conjunct} \rangle \\
& I \wedge \beta \in \mathbb{N} \wedge \forall \beta < j+1.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n \wedge k \neq 0 \\
& \wedge a[i][j] \neq 0 \\
\Rightarrow \quad & \langle \text{treating the final two conjuncts as } B \text{ in the scenario of } A \wedge B \Rightarrow A \rangle \\
& I \wedge \beta \in \mathbb{N} \wedge \forall \beta < j+1.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n \\
\Leftrightarrow \quad & \langle \text{definition of } J \text{ and substitution} \rangle \\
& J[^{j+1}/_j]
\end{aligned}
$$

To further explain the implication step, in the line above we treat

$$I \wedge \beta \in \mathbb{N} \wedge \forall \beta < j + 1.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n$$

as A and

$$k \neq 0 \wedge a[i][j] \neq 0$$

as B such that $A \wedge B \Rightarrow A$ which is true by the definition of logical implications.

2.4 Fourth implication: $J \wedge (k = 0 \vee a[i][j] = 0 \vee a[i][j] \neq b[k-1][j])$ $\wedge (k = 0 \vee a[i][j] \neq b[k-1][j]) \Rightarrow K[^0/_j]$

$$\begin{array}{ll}
& J \wedge (k = 0 \vee a[i][j] = 0 \vee a[i][j] \neq b[k-1][j]) \wedge (k = 0 \vee a[i][j] \neq b[k-1][j]) \\
\Rightarrow & \quad \langle \text{the two groups of conjuncts form an } (A \vee B \vee C) \wedge (A \vee C) \Rightarrow (A \vee C) \text{ scenario} \rangle \\
& J \wedge (k = 0 \vee a[i][j] \neq b[k-1][j]) \\
\Leftrightarrow & \quad \langle \text{definition of J} \rangle \\
& I \wedge \beta \in \mathbb{N} \wedge \forall \beta < j.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i][j] \neq b[k-1][j]) \\
\Leftrightarrow & \quad \langle \text{definition of non-equal strings* applied to the final conjunct} \rangle \\
& I \wedge \beta \in \mathbb{N} \wedge \forall \beta < j.\, (a[i][\beta] = b[k-1][\beta]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
\Rightarrow & \quad \langle \text{discard the 2nd and 3rd conjuncts and add our vacuously true statement} \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < 0.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
\Leftrightarrow & \quad \langle \text{definition of } K \text{ and substitution} \rangle \\
& K[^0/_j]
\end{array}$$

*Definition of Non-Equal Strings: a[i]$\neq$ b[j] if $\exists k\, (a[i][k] = 0) \wedge \exists l \leq k\, (a[i][l] \neq b[j][l])$

2.5 Fifth implication: $K \wedge a[i][j] \neq 0 \Rightarrow K[^{j+1}/_j][^{b:k \mapsto j \mapsto a[i][j]}/_b]$

$$
\begin{aligned}
& K \wedge a[i][j] \neq 0 \\
\Leftrightarrow \quad & \langle \text{definition of } K \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i][j] = 0 \vee a[i] \neq b[k-1]) \\
& \wedge a[i][j] \neq 0 \\
\Leftrightarrow \quad & \langle \text{the final conjunct disagrees with the sixth conjunct} \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i][j] \neq 0 \\
\Rightarrow \quad & \langle \text{treating the final conjunct as } B \text{ in the scenario of } A \wedge B \Rightarrow A \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
\Leftrightarrow \quad & \langle \text{we add a trivially true conjunct to the end of our assertion} \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
& \wedge a[i][j] = a[i][j] \\
\Leftrightarrow \quad & \langle \text{definition of } K\text{, substitutions and extracting the '}j+1\text{th' case from the 3rd conjunct} \rangle \\
& K[^{j+1}/_j][^{b:k \mapsto j \mapsto a[i][j]}/_b]
\end{aligned}
$$

2.6 Sixth implication:

$K \wedge a[i][j] = 0 \Rightarrow K[^{j+1}/_j][^{b:k \mapsto j \mapsto 0}/_b]$

$$
\begin{aligned}
& K \wedge a[i][j] = 0 \\
\Leftrightarrow \quad & \langle \text{definition of } K \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
& \wedge a[i][j] = 0 \\
\Leftrightarrow \quad & \langle \text{the last conjunct is trivially the same in reverse order} \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
& \wedge 0 = a[i][j] \\
\Leftrightarrow \quad & \langle \text{definition of } K\text{, substitutions and extracting the '}j+1\text{th' case from the 3rd conjunct} \rangle \\
& K[^{j+1}/_j][^{b:k \mapsto j \mapsto 0}/_b]
\end{aligned}
$$

2.7 Seventh implication: $K \Rightarrow I[^{i+1}/_i][^{k+1}/_k] \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i] = b[k]$

$$
\begin{aligned}
& K \\
\Leftrightarrow \quad & \langle \text{definition of } K \rangle \\
& I \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
\Leftrightarrow \quad & \langle \text{definition of } I \rangle \\
& \alpha \in \mathbb{N} \wedge \forall \alpha < i.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq i \leq n \wedge m(i) = k \wedge a_0 = a \wedge n_0 = n \\
& \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
\Leftrightarrow \quad & \langle \text{simplifying the 3rd and 10th conjunct} \rangle \\
& \alpha \in \mathbb{N} \wedge \forall \alpha < i.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq i < n \wedge m(i) = k \wedge a_0 = a \wedge n_0 = n \\
& \wedge \gamma \in \mathbb{N} \wedge \forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma]) \wedge (k = 0 \vee a[i] \neq b[k-1]) \\
\Rightarrow \quad & \langle \text{using proofs 'Proof 1'* and 'Proof 2'**} \rangle \\
& \alpha \in \mathbb{N} \wedge \forall \alpha < i.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq i < n \wedge m(i+1) = k+1 \wedge a_0 = a \wedge n_0 = n \\
& \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i] = b[k] \wedge a[i] = b[m(i)] \\
\Leftrightarrow \quad & \langle \text{expanding the 3rd conjunct into two separate (3rd and 7th conjuncts below)} \rangle \\
& \alpha \in \mathbb{N} \wedge \forall \alpha < i.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq i+1 \leq n \wedge m(i+1) = k+1 \wedge a_0 = a \wedge n_0 = n \\
& \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i] = b[k] \wedge a[i] = b[m(i)] \\
\Leftrightarrow \quad & \langle \text{reducing the '}i+1\text{th' case} \rangle \\
& \alpha \in \mathbb{N} \wedge \forall \alpha < i+1.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq i < n \wedge m(i+1) = k+1 \wedge a_0 = a \wedge n_0 = n \\
& \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i] = b[k] \\
\Leftrightarrow \quad & \langle \text{definition of } I \text{ and substitutions} \rangle \\
& I[^{i+1}/_i][^{k+1}/_k] \wedge 0 \leq i < n \wedge (k = 0 \vee a[i] \neq b[k-1]) \wedge a[i] = b[k]
\end{aligned}
$$

*Proof 1: We need to prove that $m(i+1) = k+1$ is a true statement. To do so

**Proof 2: We need to prove that $a[i] = b[m(i)]$ is a true statement. To do so we remember that at this part of the program, we have just passed the 'Fifth Implication' in which we proved $b[k][j] = a[i][j]$ by using the conjunct of K in which specifically

$\forall \gamma < j.\, (b[k][\gamma] = a[i][\gamma])$

We define 'Equal Strings' to be

$a[i] = b[j]$ if $\exists k\, (a[i][k] = 0) \wedge \forall l \leq k\, (a[i][l] = b[j][l])$

and this follows on from our definition of K. The final two conjuncts are

$a[i] = b[k] \wedge a[i] = b[m(i)]$

Furthermore, we know from our definition of our m index mapping function that $m(i) = k$. Hence, these two conjuncts prove that

$a[i] = b[m(i)]$.

2.8 Eighth implication:

$I[^{i+1}/_i] \wedge 0 \leq i < n \Rightarrow I[^{i+1}/_i]$

$$
\begin{array}{ll}
 & I[^{i+1}/_i] \wedge 0 \leq i < n \\
\Rightarrow & \quad \langle \text{treating the final conjunct as } B \text{ in the scenario of } A \wedge B \Rightarrow A \rangle \\
 & I[^{i+1}/_i]
\end{array}
$$

2.9 Ninth implication:

$I \wedge i \geq n \Rightarrow \alpha \in \mathbb{N} \wedge \forall \alpha < n.\, (a[\alpha] = b[m(\alpha)]) \wedge m(n) = k \wedge a = a_0 \wedge n = n_0$

$$
\begin{array}{ll}
 & I \wedge i \geq n \\
\Leftrightarrow & \quad \langle \text{definition of } I \rangle \\
 & \alpha \in \mathbb{N} \wedge \forall \alpha < i.\, (a[\alpha] = b[m(\alpha)]) \wedge 0 \leq i \leq n \wedge m(i) = k \wedge a_0 = a \wedge n_0 = n \wedge i \geq n \\
\Leftrightarrow & \quad \langle \text{simplify the third and last conjunct to } i = n \rangle \\
 & \alpha \in \mathbb{N} \wedge \forall \alpha < n.\, (a[\alpha] = b[m(\alpha)]) \wedge m(n) = k \wedge a_0 = a \wedge n_0 = n
\end{array}
$$

Through logical equivalence, it is obvious that logical implication exists in both directions.

3 Task 3

```c
#include <stdio.h>
#include <assert.h>
#include <string.h>
#include "uniq.h"

unsigned int uniq(unsigned int n, char *a[], char *b[]) {
    int i, k = 0;

    for (i = 0; i < n; i++) {
        if (k == 0 || (strcmp(a[i], b[k-1]) != 0)) {
            strcpy(b[k], a[i]);
            k++;
        }
    }
```

```
    return k;
}
```

In our C implementation, we opted for the more traditional **for** loop idiom instead of a **while** loop. It should be clear that our **for** loop captures the meaning of the encapsulating **while** loop of the toy language program. We used a call of the C library function strcmp to implement the first nested **while** loop (pseudo-code ”$j = j + 1$”) and the second **if** condition (pseudo-code ”$a[i][j] - b[k-1][j] \neq 0$”) that compares the values in array $a[i]$ to array $b[j]$. (Cf. man strcmp.)

As for the second nested **while** loop (pseudo-code ”$b[k][j] = a[i][j]$”), we used a call of the C library function strcpy to copy the contents of array $b[k]$ to $a[i]$. (Cf. man strcpy.) Due to the conversion to the C functions strcmp and strcpy, this means the integer variable j is unused by the program and can be removed from the C code.