Hans Weeks and Christina Yu
Software Specifications
September 24, 2017

Homework 4

In the following proof we show that program specified in assignment 3 meets the specification from assignment 2. Namely, that a matrix with 1 color and 1 label per element will eventually have each color-region with a matching label unique to that region. We do this by introducing 2 invariants, then showing that init leads to post using a well founded metric. Then we show that once we have reached post, the program does not change.

Invariant 1: $\langle \exists x : \pi(x) :: L(x) \neq \lambda(x) \ \rangle$
Let x = (i,j) and y = (p,q)
Initially, L(i, j) = (i, j). There is a label which is smaller than every other labels in the same region.
Furthermore, assume "if SameRegion((i,j),(p,q))" is true,
the statement L(i,j):= min(L(i,j),L(p,q)) ensures L(y)=$\lambda(y)$=$\lambda(x)$
Thus, there always exists a cell x whose label is $\lambda(x)$.

Invariant 2: $\langle \forall x, y : \pi(x) \wedge \pi(y) \wedge \neg(x\Gamma y) :: L(x) \neq L(y) \ \rangle$
Let x = (i,j) and y = (a,b)
Initially, $L(x) = (i,j) \wedge L(y) = (a,b) \wedge (i,j) \neq (a,b) \implies L(x) \neq L(y)$
which means cell x and y have different initial labels.
Furthermore, there exists the statement S_{ijpq} ensures L(x)=$\lambda(x)$ and a statement S_{abcd} ensures L(y)=$\lambda(y)$.
$if \neg(x\Gamma y)$ is true, then $\lambda(x) \neq \lambda(y)$, $\implies$ L(x) $\neq$ L(y)
when L(x) $\neq$ L(y), none of the assignment alter the state.

1. init $\rightsquigarrow$ post
   let's define μ:
   $\mu = \langle \ \Sigma \ \forall \ x : \pi(x) :: L(x) \neq \lambda(x) \ \rangle$
   This is well founded because initially only 1 element per region is correctly labeled.

   With this μ in mind, we would like to show 2 things:
   1. μ only decreases and 2. when $\mu = 0$, then we have reached post.

   Part 1:

   $$\mu = k \rightsquigarrow \mu < k$$

   μ increases or stays the same. If k is 0, then it never decreases, just remains 0. If k is greater than 0, then there exists a statement S_{ijpq} where

(i, j) is an element that does not have its final label and (p, q) does have its final label. Then

$$S_{ijpq} \; ensures \; \mu < k$$

By invariant 1 we know that such an element pq always exists.

Part2:

$$\mu = 0 \implies post$$

First, if the number of elements that don't have there final label is equal to zero, then all elements must have there final label
$\checkmark\ \mu = 0 \implies \langle \forall x : \pi(x) :: L(x) = \lambda(x) \rangle$

Second, if we have 2 elements that are not in the same region but have the same label, that implies that one of those elements does not have its final label:

$$L(x) = L(y) \wedge \neg(x\Gamma y) \implies L(x) \neq \lambda(x) \vee L(y) \neq \lambda(y)$$

which implies that $\mu(x) > 0$
therefore
$\checkmark \mu(x) = 0 \implies \langle \forall x, y \; : \pi(x) \; \wedge \pi(x) \wedge \neg(x\Gamma y) :: \; L(x) \neq L(x) \; \rangle$

2. **stable** post

$post \equiv \langle \forall x \ : \ \pi(x) \ :: \ L(x) = \lambda(x) \ \rangle$
$\wedge \ \langle \forall x, y \ : \pi(x) \ \wedge \pi(x) \wedge \neg(x\Gamma y) :: \ L(x) \neq L(x) \ \rangle$

$part1 : post \equiv \langle \forall x \ : \ \pi(x) \ :: \ L(x) = \lambda(x) \ \rangle$
$Let \ x = (i, j) \ and \ y = (p, q)$
$There \ exists \ the \ statement \ S_{ijpq} \ ensures L(x) = \lambda(x) \ and$
$a \ statement \ S_{abcd} \ ensures \ L(y) = \lambda(y).$
$Assume \ \text{``}if \ SameRegion((i, j), (p, q))'' \ is \ true, \ which \ means \ x \ \rho \ y.$
$then \ \lambda(x) = \lambda(y) \implies L(x) = L(y) = \lambda(x) = \lambda(y)$
$which \ means \ all \ cells \ in \ the \ same \ region \ share \ the \ same \ final \ label.$
$And \ once \ L(x) = L(y) = \lambda(x) = \lambda(y), \ none \ of \ the \ assignment \ alter \ the \ state.$

$part2 : \langle \forall x, y : \pi(x) \ \wedge \ \neg(x\Gamma y) :: L(x) \neq L(y) \rangle$
$It \ is \ the \ invariant2 \ proved \ on \ page \ 1.$