CS 580 Specification of Software Systems

Homework 05: Formal properties. Consider a square matrix B of size N. Let A represent the initial configuration of the matrix B.

(1) Write a UNITY program that transposes the rows and columns of matrix B and preserves the following invariant:

inv. $p \leq q \wedge$

$$\langle \forall\, i,j : (1 \leq i < p \vee 1 \leq j < p \vee q < i \leq N \vee q < j \leq N) \wedge 1 \leq i \leq N \wedge 1 \leq j \leq N :: B[i, j] = A[j, i] \rangle$$

Program Transpose

declare

A: array of[1…N, 1…N] of integer

p, q: integer

initially

A = B

$p = 2 \wedge q = N\text{-}1$

assign

s1 $\langle \| \; i,j : 1 \leq i, j < p :: A[i, j] := B[j, i] \rangle$

$\|$

s2 $\langle \| \; i,j : q < i, j \leq N :: A[i, j] := B[j, i] \rangle$

$\|$

s3 $p := p+1 \wedge q := q\text{-}1$ if $p \leq q$

end

(2) Write a formal specification of the correctness of the program you designed. Such a specification often assumes the following general form:

a. init —> Post

b. stable Post

Init: $B = \Gamma = A \wedge p \leq q$

Post: $B = \Gamma \wedge p \leq q \wedge$

$\langle \forall\ i,j : (1 \leq i < p \vee 1 \leq j < p \vee q < i \leq N \vee q < j \leq N) \wedge 1 \leq i \leq N \wedge 1 \leq j \leq N :: A[i, j] = B[j, i] \rangle$

// slightly modified from Inv.

(3) Explain in narrative form (no formal proof) the steps involved in proving these two properties.

$\pi(x) = < \exists\ i, j : x = (i, j) :: 1 \leq i, j \leq N >$

$T(x) = < \exists\ x : \pi(x) : A[x] := B[x] >$

init —> post:

Let $\mu = < \Sigma\ x : \neg\ T(x) :: 1>$, the number of cells have not been transposed.

s1 ensures a region starting from the top left corner of board B is transposed. The region starts with one cell(1, 1).

s2 ensures a region starting from the bottom right corner of board B is transposed. The region starts with one cell(N, N).

s3 ensures the two regions add more cells to it, which means μ decreases.