

## 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:

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

### Program Transpose

#### declare

$A$ : array of  $[1 \dots N, 1 \dots N]$  of integer  
 $p, q$ : integer

#### initially

$A = B$   
 $p = 2 \wedge q = N - 1$

#### assign

$\langle [] i, j : 1 \leq i, j < p :: A[i, j] = B[j, i] \rangle$   
 $\parallel$   
 $\langle [] i, j : q < i, j \leq N :: A[i, j] = B[j, i] \rangle$   
 $\parallel$   
 $p := p + 1 \wedge q := q - 1 \text{ if } p \leq q$

#### end

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

- a.  $\text{init} \rightarrow \text{Post}$
- 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.

$\text{init} \rightarrow \text{post}$ :

Let  $\mu = \langle \rangle$