**3.3.7.14**

Consider the following code segment that swaps the contents of b(i) and b( j). Prove it correct. {Q: 1 ≤ i ≤ j ≤ n ∧ (∀k | 1 ≤ k ≤ n : b(k) = c(k)) }

t := b(i)

b(i) := b(j)

b(j) := t

{R: 1 ≤ i ≤ j ≤ n ∧ (∀k | 1≤ k ≤ n ∧ k != i ∧ k != j : b(k) = c(k)) ∧ b(i) = c(j) ∧ b(j) = c(i)}

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<code segment is correct iff>

Q ⇒ wp(t := b(i) ; b(i) := b(j) ; b(j) := t ; R)

<Composition>

Q ⇒ wp(t := b(i) ; b(i) := b(j) ; wp(b(j) := t , R))

<Expanding R>

Q ⇒ wp(t := b(i) ; b(i) := b(j) ; wp(b(j) := t , 1 ≤ i ≤ j ≤ n ∧ (∀k | 1≤ k ≤ n ∧ k != i ∧ k != j : b(k) = c(k)) ∧ b(i) = c(j) ∧ b(j) = c(i)))

<Replacing b(j) with t>

Q ⇒ wp(t := b(i) ; b(i) := b(j) ; ( 1 ≤ i ≤ j ≤ n ∧ (∀k | 1≤ k ≤ n ∧ k != i ∧ k != j : b(k) = c(k)) ∧ b(i) = c(j) ∧ t = c(i)))

<Composition>

Q ⇒ wp(t := b(i) , wp(b(i) := b(j) , ( 1 ≤ i ≤ j ≤ n ∧ (∀k | 1≤ k ≤ n ∧ k != i ∧ k != j : b(k) = c(k)) ∧ b(i) = c(j) ∧ t = c(i))))

<Replacing b(i) with b(j)>

Q ⇒ wp(t := b(i) , ( 1 ≤ i ≤ j ≤ n ∧ (∀k | 1≤ k ≤ n ∧ k != i ∧ k != j : b(k) = c(k)) ∧ b(j) = c(j) ∧ t = c(i)))

<replacing t with b(i)>

Q ⇒ ( 1 ≤ i ≤ j ≤ n ∧ (∀k | 1≤ k ≤ n ∧ k != i ∧ k != j : b(k) = c(k)) ∧ b(j) = c(j) ∧ b(i) = c(i))

<Expanding Q>

(1 ≤ i ≤ j ≤ n ∧ (∀k | 1 ≤ k ≤ n : b(k) = c(k))) ⇒ ( 1 ≤ i ≤ j ≤ n ∧ (∀k | 1≤ k ≤ n ∧ k != i ∧ k != j :

b(k) = c(k)) ∧ b(j) = c(j) ∧ b(i) = c(i))

<by definition / It’s obvious >

T

**3.3.8.15 (2. only, but look at all three)**

Prove that (p⇒(q⇒r)) ⇔ ((p∧q)⇒r))

(p⇒(q⇒r)) <=>

(Implication Law) (p⇒(¬ q ∨ r )) <=>

(Implication Law) (¬ p ∨ (¬ q ∨ r )) <=>

(De Morgan’s Law) ¬ (p ∧ (q ∧ ¬ r )) <=>

(Associativity Law) ¬ ((p ∧ q) ∧ ¬ r ) <=>

(De Morgan’s Law) (¬(p ∧ q) ∨ r) <=>

(Implication Law) ((p ∧ q) => r )

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.3.8.16**

{T}

if

x ≥ y → m := x

x ≤ y → m := y

endif

{m = max(x, y)}

P ⇒ (G0 ∨ G1) ⇔ <instantiate>

T ⇒ (x ≥ y ∨ x ≤ y) ⇔ <Excluded middle >

T

P∧G0 ⇒ wp(S0,Q) ⇔ <instantiate>

(T ∧ x ≥ y) ⇒ wp(“m := x”, m = max(x, y)) ⇔ <definition of := / ∧-simplification>

(x ≥ y) ⇒ x = max(x, y) ⇔ <algebra>

T

P∧G1 ⇒ wp(S1,Q)

(T ∧ x ≤ y) ⇒ wp(“m := x”, m = max(x, y)) ⇔ <definition of := / ∧-simplification>

(x ≤ y) ⇒ x = max(x, y) ⇔ <algebra>

T

**3.3.8.17**

{ ( ∀j | 1≤ j<i : m≤b(j) ) }

if

b(i) ≥ m → skip

b(i) ≤ m → m := b(i)

endif

i:=i+1

{ ( ∀j | 1 ≤ j ≤ i : m ≤ b(j) ) }

Q = wp(“i := i + 1”, R) = R (i to i+1) = (∀j | 1 ≤ j≤ i : m ≤ b(j)) (i to i+1) = (∀j|1≤ j≤ i+1:m≤ b(j))

P ⇒ (G0 ∨ G1) ⇔ <instantiate>

( ∀j | 1 ≤ j ≤ i : m ≤ b(j) ) ⇒ (b(i) ≥ m ∨ b(i) ≤ m) ⇔ <Excluded middle >

( ∀j | 1 ≤ j ≤ i : m ≤ b(j) ) ⇒ T ⇔ <Implication Law>

T

P∧G0 ⇒ wp(S0,Q) ⇔ <instantiate>

(∀j | 1 ≤ j ≤ i : m ≤ b(j)) ∧ b(i) ≥ m ⇒ wp(skip , (∀j|1≤ j≤ i+1:m≤ b(j))) ⇔ <definition of skip>

(∀j | 1 ≤ j ≤ i : m ≤ b(j)) ∧ b(i) ≥ m ⇒ (∀j|1≤ j≤ i+1:m≤ b(j)) <algebra>

T

P∧G1 ⇒ wp(S1,Q)

(∀j|1≤ j≤ i:m ≤ b(j)) ∧ b(i) ≤ m ⇒ wp(m := b(i) , (∀j|1≤ j≤ i+1:m≤ b(j))) ⇔ <definition of :=>

(∀j|1≤ j≤ i:m ≤ b(j)) ∧ b(i) ≤ m ⇒ (∀j|1≤ j≤ i+1:b(i) ≤ b(j)) ⇔ <algebra>

**3.3.8.18**

The following code segment might be part of a loop that computes the maximum value *m* in array *b*(1 : *n*) as well as the index *i* such that *b*(*i*) = *m*. Prove it correct.

{P: (1≤i<k<n) ∧ b(i) = m ∧ (∀j|1≤ j<k:b(j)≤m)}

if

b(k) ≥ m → m := b(k) ; i := k

b(k) ≤ m → skip

Endif

**{Q}**

k := k + 1

{R: (1≤i<k≤n) ∧ b(i) = m ∧ (∀j| 1 ≤ j < k: b(j) ≤ m)}

Proof:

Q = wp(“k := k + 1” , R) = R ( k to k+1) =

(1 ≤ i < k ≤ n) ∧ b(i) = m ∧ (∀j| 1 ≤ j < k: b(j) ≤ m)( i to i+1)

(1 ≤ i < k + 1 ≤ n) ∧ b(i) = m ∧ (∀j| 1 ≤ j < k + 1: b(j) ≤ m)

P ⇒ (G0 ∨G1) ⇔ < instantiate >

P ⇒ (b(k) ≥ m ∨ b(k) ≤ m) ⇔ < Excluded middle >

P⇒T ⇔ < definition of ⇒ >

T

P∧G0 ⇒ wp(S0,Q) ⇔ < instantiate >

P∧G0 ⇒ wp( m := b(k) , wp( i := k , (1≤i<k+1≤n) ∧ b(i) = m ∧ (∀j| 1 ≤ j < k+1: b(j) ≤ m)))

⇔ < definition := >

P∧G0 ⇒ wp( m := b(k) , (1≤k<k+1≤n) ∧ b(k) = m ∧ (∀j| 1 ≤ j < k+1: b(j) ≤ m))

⇔ < definition := >

P∧G0 ⇒ (1≤k<k+1≤n) ∧ b(k) = b(k) ∧ (∀j| 1 ≤ j < k+1: b(j) ≤ b(k)))

⇔ < identity >

P∧G0 ⇒ (1≤k<k+1≤n) ∧ (∀j| 1 ≤ j < k+1: b(j) ≤ b(k)))

⇔ < instantiate >

(1≤i<k<n) ∧ b(i) = m ∧ (∀j|1≤ j<k:b(j)≤m) ∧ b(k) ≥ m ⇒

(1≤k<k+1≤n) ∧ (∀j| 1 ≤ j< k+1: b(j) ≤ b(k))) ⇔ < algebra >

(1≤i<k<n) ∧ b(i) = m ⇒ (1≤k<k+1≤n) ⇔ < algebra / weakening - strengthening>

T

P∧G1 ⇒ wp(S1,Q):

P∧G1 ⇒ wp(S1,Q) ⇔ < instantiate >

P∧G1 ⇒ wp( skip , ((1 ≤ i < k+1 ≤ n) ∧ b(i) = m ∧ (∀j| 1 ≤ j < k+1: b(j) ≤ m))

⇔ < definition of skip >

P∧G1 ⇒ ((1 ≤ i< k+1 ≤ n) ∧ (b(i) = m) ∧ (∀j| 1 ≤ j < k+1: b(j) ≤ m)) ⇔ < instantiate >

(1 ≤ i < k < n) ∧ (b(i) = m) ∧ (∀j | 1≤ j < k : b(j) ≤ m) ∧ (b(k) ≤ m) ⇒

((1 ≤ i < k+1 ≤ n) ∧ (b(i) = m) ∧ (∀j | 1 ≤ j < k+1: b(j) ≤ m)) ⇔ < algebra/identity/ >

(∀j | 1≤ j < k : b(j) ≤ m) ∧ (b(k) ≤ m) ⇒ (∀j | 1 ≤ j < k+1: b(j) ≤ m) ⇔ <algebra>

T