Syntactic Substitution, Forward Assignment, & sp

CS 536: Science of Programming, Fall 2022

HW 6 Solution

Class 12: Syntactic Substitutions [30 points]

For Problems 1 – 4, p ≡ x*y < f(a) ∨ ∃ x . x ≥ a*y → ∃ y . f(x*y) > a-y+z

1. p[y+z/x]
   ≡ (x*y < f(a) ∨ ∃ x . x ≥ a*y → ∃ y . f(x*y) > a-y+z) [y+z/x]
   ≡ (y+z)*y < f(a) ∨ ∃ x . x ≥ a*y → ∃ y . f(x*y) > a – y+z // The other x's are bound

2. p[a – y/y]
   ≡ (x*y < f(a) ∨ ∃ x . x ≥ a*y → ∃ y . f(x*y) > a – y+z) [a–y/y]
   ≡ x*(a–y) < f(a) ∨ ∃ x . x ≥ a*(a–y) → ∃ y . f(x*y) > a –y+z // The other y's are bound

3. p[a*y/a]
   ≡ (x*y < f(a) ∨ ∃ x . x ≥ a*y → ∃ y . f(x*y) > a – y+z) [a*y/a]
   ≡ (x*y < f(a) ∨ ∃ x . x ≥ a*y → ∃ y_1 . f(x*y_1) > a – y_1+z) [a*y/a] // renaming y to avoid capture
   ≡ x*y < f(a*y) ∨ ∃ x . x ≥ (a*y)*y → ∃ y_1 . f(x*y_1) > (a*y) – y_1+z

4. p[x÷y/a][y – z/x]
   ≡ (x*y < f(a) ∨ ∃ x . x ≥ a*y → ∃ y . f(x*y) > a – y+z) [x÷y/a] [y – z/x]
   ≡ (x*y < f(a) ∨ ∃ x_1 . x_1 ≥ a*y → ∃ y_1 . f(x_1*y_1) > a – y_1+z) [x÷y/a] [y – z/x]
   // rename x and y to avoid capture
   ≡ (x*y < f(x÷y) ∨ ∃ x_1 . x_1 ≥ (x÷y)*y → ∃ y_1 . f(x_1*y_1) > x÷y – y_1+z) [y – z/x]
   // 1st substitution
   ≡ (y – z)*y < f((y – z)÷y) ∨ ∃ x_1 . x_1 ≥ ((y – z)÷y)*y → ∃ y_1 . f(x_1*y_1) > (y – z)÷y – y_1+z
   // 2nd substitution

Lecture 13: Forward Assignment; Strongest Postconditions [30 points]

5. (S such that ⊨ {T} S {sp(T, S)} but ⊭$_{tot}$ {T} S {sp(T, S)})
   By definition, a final state for S is always part of the sp, so only nontermination makes us not have total correctness with the sp. Examples include a diverging loop such as ***while true do skip od*** or code with a runtime error, such as {T} x := 1/0; x := 2 {x = 2}.

6. (Calculate $sp(x < y \wedge x+y \le n,\ x := f(x+y);\ y := g(x*y)))$

   First, let's calculate $sp(x < y \wedge x+y \le n,\ x := f(x+y)) \equiv x_0 < y \wedge x_0+y \le n \wedge x = f(x_0+y)$, so then

   $sp(x < y \wedge x+y \le n,\ x := f(x+y);\ y := g(x*y))$

   $\equiv sp(sp(x < y \wedge x+y \le n,\ x := f(x+y)),\ y := g(x*y))$

   $\equiv sp(x_0 < y \wedge x_0+y \le n \wedge x = f(x_0+y),\ y := g(x*y))$

   $\equiv x_0 < y_0 \wedge x_0+y_0 \le n \wedge x = f(x_0+y_0) \wedge y = g(x*y_0)$ // Note $g(x, \ldots)$ not $g(x_0, \ldots)$

7. (Calculate and logically simplify)

   $sp(x = 2\hat{}k,\ x := x/2) \equiv x_0 = 2\hat{}k,\ x = x_0/2$. Simplifying, we get $2*x = 2\hat{}k$, so $x = 2\hat{}(k-1)$

8. (Calculate but don't simplify)

   $wp(x := x/2,\ x = 2\hat{}k) \equiv (x = 2\hat{}k)[x/2 \,/\, x] \equiv x/2 = 2\hat{}k$

9. (For $S \equiv$ ***if*** even(x) ***then*** x := x+1 ***fi***)

   9a. (Calculate and simplify)

   wp(S, odd(x))

   ≡ wp(***if*** even(x) ***then*** x := x+1 ***fi***, odd(x)) // defn S

   ≡ wp(***if*** even(x) ***then*** x := x+1 ***else skip fi***, odd(x)) // defn ***if-then***

   ≡ (even(x) → wp(x := x+1, odd(x))) ∧ (odd(x) → wp(***skip***, odd(x))) // wp of ***if-else***

   ≡ (even(x) → odd(x+1)) ∧ (odd(x) → odd(x))

   ⇔ T

   9b. (Calculate and simplify, dropping x_0)

   $sp(x = x_0, S)$

   ≡ sp($x = x_0$, ***if*** even(x) ***then*** x := x+1 ***else skip fi***)

   ≡ sp($x = x_0 \wedge$ even(x), x := x+1) ∨ sp($x = x_0 \wedge$ odd(x), ***skip***) // sp of ***if-else***

   ≡ (even(x_0) ∧ $x = x_0+1$) ∨ ($x = x_0$ ∧ odd(x))

   ⇒ odd(x)

10. (Binary search S ≡ ***if*** x < b[mid] ***then*** right ***:=*** mid ***else*** left ***:=*** mid ***fi***)

    10a. (Calculate only). Given $p \equiv left < right-1 \wedge mid = (left + right)/2 \wedge b[left] \le x < b[right]$ and $p' \equiv left = left_0 \wedge right = right_0$,

    $sp(p \wedge p', S)$

    ≡ sp(p ∧ p′, ***if*** x < b[mid] ***then*** right := mid ***else*** left := mid ***fi***)

    $\equiv q_1 \vee q_2$ where $q_1 \equiv sp(p \wedge p' \wedge x < b[mid],\ right := mid)$

    and $q_2 \equiv sp(p \wedge p' \wedge x \ge b[mid],\ left := mid)$

Then $q_1 \equiv sp(p \wedge p' \wedge x < b[mid], right := mid)$

$\equiv sp(left < right - 1 \wedge mid = (left + right)/2 \wedge b[left] \le x < b[right]$
$\wedge\ left = left_0 \wedge right = right_0 \wedge x < b[mid], right := mid\ )$

$\equiv (left < right_0 - 1 \wedge mid = (left + right_0)/2 \wedge b[left] \le x < b[right_0]$
$\wedge\ left = left_0 \wedge x < b[mid] \wedge right = mid\ )$

And $q_2 \equiv sp(p \wedge p' \wedge x \ge b[mid], left := mid)$

$\equiv sp(left < right - 1 \wedge mid = (left + right)/2 \wedge b[left] \le x < b[right]$
$\wedge\ left = left_0 \wedge right = right_0 \wedge x \ge b[mid], left := mid\ )$

$\equiv left_0 < right - 1 \wedge mid = (left_0 + right)/2 \wedge b[left_0] \le x < b[right]$
$\wedge\ right = right_0 \wedge x \ge b[mid] \wedge left = mid$

10b. (Calculate only) Again, $p' \equiv left = left_0 \wedge right = right_0$, but this time let
$p \equiv -1 \le left-1 \le right \wedge mid = (left + right)/2 \wedge (x \in b[0...n-1] \leftrightarrow x \in b[left..right])$.

Then $sp(p \wedge p', S)$

$\equiv sp(p \wedge p'$, ***if*** $x < b[mid]$ ***then*** $right := mid$ ***else*** $left := mid$ ***fi***)

$\equiv q_1 \vee q_2$ where $q_1 \equiv sp(p \wedge p' \wedge x < b[mid], right := mid)$
and $q_2 \equiv sp(p \wedge p' \wedge x \ge b[mid], left := mid)$

So $q_1 \equiv sp(p \wedge p' \wedge x < b[mid], right := mid)$

$\equiv sp(-1 \le left-1 \le right \wedge mid = (left + right)/2 \wedge (x \in b[0...n-1] \leftrightarrow x \in b[left..right])$
$\wedge\ left = left_0 \wedge right = right_0 \wedge x < b[mid], right := mid\ )$

$\equiv -1 \le left-1 \le right_0 \wedge mid = (left + right_0)/2 \wedge (x \in b[0...n-1] \leftrightarrow x \in b[left..right_0])$
$\wedge\ left = left_0 \wedge x < b[mid] \wedge right = mid$

And $q_2 \equiv sp(p \wedge p' \wedge x \ge b[mid], left := mid)$

$\equiv sp(-1 \le left-1 \le right \wedge mid = (left + right)/2 \wedge (x \in b[0...n-1] \leftrightarrow x \in b[left..right])$
$\wedge\ (left = left_0 \wedge right = right_0) \wedge x \ge b[mid], left := mid\ )$

$\equiv -1 \le left_0 - 1 \le right \wedge mid = (left_0 + right)/2 \wedge (x \in b[0...n-1] \leftrightarrow x \in b[left_0..right])$
$\wedge\ right = right_0 \wedge x \ge b[mid] \wedge left = mid$

