CS536 Science of Programming

HW-8

Sai Vishal Kodimela (A20453006)

Venkata Akshith Reddy Kasireddy (A20455209)

Atharva Kadam (A20467229)

Class 17: Full Proof Outlines [10 points]

1) Let $p \equiv \{1 \le k \le n \land p = n!/k!\}$

$\{n > 0\}$
$k := n-1;\ \{n > 0 \land k = n-1\}$
$p := n;\ \{n > 0 \land k = n-1 \land p = n\}$
$\{inv\ p\}$ while $k > 1$ do // where $p \equiv 1 \le k \le n \land p = n!/k!$
$\{p \land k > 1\}$
$\{p[p*k/p][k-1/k]\}$ $k:= k-1;$
$\{p[p*k/p]\}$ $p:= p*k$ $\{p\}$
od $\{p \land k \le 1\}$ $\{p = n!\}$

Substitutions:

$p[p*k/p] \equiv 1 \le k \le n \land p*k = n!/k!$

$p[p*k/p][k-1/j] \equiv 1 \le k \le n \land p*(k-1) = n!/(k-1)!$

Class 17: Partial Proof Outlines [20 points total]

4) (Full proof outline from minimal outline, using sp.)

$\{q \equiv r = X*Y-x*y\}$
if even(x) then
$\{q \land even(x)\}$
$y := 2*y;\ \{r_0 = X*Y-x*y \land even(x_0) \land y = 2*y_0\}$
$x := x/2\ \{r_0 = X*Y-x*y \land even(x_0) \land y = 2*y_0 \land x = x_0/2\}$
else
$\{q \land odd(x)\}$
$r := r+y;\ \{r_0 = X*Y-x*y \land odd(x) \land r = r_0+y\}$
$x := x-1\ \{r_0 = X*Y-x_0*y \land odd(x) \land r = r_0+y \land x = x_0-1\}$

fi $\{q\}$

5) (Full proof outline from minimal outline, using wp.)

$\{y \geq 1\}$ x := 0; r := 1;
$\{\text{inv } p \equiv 1 \leq r = 2\text{^}x \leq y\}$ while $2*r \leq y$ do
  $\{p \wedge 2*r \leq y\}$
  $\{1 \leq 2*r = 2\text{^}(x+1) \leq y\}$ r := 2*r;
  $\{1 \leq r = 2\text{^}(x+1) \leq y\}$ x := x+1
  $\{p\}$

od $\{p \wedge 2*r > y\}$ $\{r = 2\text{^}x \leq y \leq 2\text{^}(x+1)\}$

Class 18: Convergence [20 points total]

1) (Bound expression for {inv p} {bd t } while k ≤ n do … k := k+1 od)
   a) n-k is invalid: It can be negative; n-k is decreased by the loop body.
   b) n+k+C is invalid: Incrementing k does not decrease it; n+k+C is nonnegative.
   c) n-k+C is valid: Incrementing k decreases it; we know j ≤ n+C, which implies n-k+C ≥ 0.
   d) n-k+2*C is valid. Incrementing k decreases it, and since C > 0, we know that
      n-k+ 2*C > n-k+C ≥ 0.
   e) 2^(n+C)/2^k is valid. Incrementing k decreases it and k ≤ n+C, implies 2^k ≤ 2^(n+C)

2) $\{b[c] \geq 1 \wedge 0 \leq c < |b|\}$ // call this p_0
x := 1;
$\{ p_0 \wedge x = 1\}$ // (sp of line above)
k := 0;
$\{p_0 \wedge x = 1 \wedge k = 0\}$ // (sp of line above)
$\{\text{inv } p \equiv x = 2\text{^}k \leq b[c]\}$
  $\wedge\ 0 \leq c < |b| \wedge b[c]\text{-}x > 0\}$ // (Augment p to ensure bound expression ≥ 0)
{bd b[c]-x} // (other bounds include b[j]-k, ceil($\log_2$(b[j]))-k)
while 2*x ≤ b[c] do
  $\{p \wedge 2*x \leq b[c] \wedge b[c]\text{-}x = t_0\}$ // (let t_0 be value of bound expr at top of loop body)
  $\{p[2*x/x][k+1/k] \wedge b[c]\text{-}2*x < t_0\}$ // (Add wp of the assignment below.)
  k := k+1;
  $\{p[2*x/x] \wedge b[c]\text{-}2*x < t_0\}$ // (Add wp of the assignment below.)
  x := 2*x
  $\{p \wedge b[c]\text{-}x < t_0\}$ // (Add bound expr < logical variable.)

od

$\{p \wedge 2*x > b[c]\}$

$\{x = 2\text{^}k \leq b[c] < 2\text{^}(k+1)\}$