Solution to Homework 8

Classes 16 & 17: Proof Outlines

1. (Full outline from formal proof)

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

2. (Expand partial outline)

$\{y \ge 1\}$
$\{p[1/r][0/x]\}\ x := 0\,;$ // $p[1/r][0/x] \equiv 1 \le 1 = 2\,\hat{}\,0 \le y$
$\{p[1/r]\}\ r := 1\,;$ // $p[1/r] \equiv 1 \le 1 = 2\,\hat{}\,x \le y$
$\{\textbf{inv}\ p \equiv 1 \le r = 2\,\hat{}\,x \le y\}$
while $2*r \le y$ ***do***
  $\{p \wedge 2*r \le y\}$
  $\{p[x+1/x][2*r/r]\}\ r := 2*r\,;$ // $p[x+1/x][2*r/r] \equiv 1 \le 2*r = 2\,\hat{}\,(x+1) \le y$
  $\{p[x+1/x]\}\ x := x+1$ // $p[x+1/x] \equiv 1 \le r = 2\,\hat{}\,(x+1) \le y$
  $\{p\}$
od
$\{p \wedge 2*r > y\}$
$\{r = 2\,\hat{}\,x \le y \le 2\,\hat{}\,(x+1)\}$

Class 18: Total Correctness

3. (Convergence of $\{\textbf{inv}\ p\}\{\textbf{bd}\ t\}$ ***while*** B ***do*** S ***od*** $\{p \wedge \neg B\}$)

   a. Must be true: $\{p \wedge B \wedge t > t_0\}\ S\ \{t = t_0\}$. Whatever t is at the end of the iteration; it needed to be larger at the start of the iteration.

   b. Must be true: $p \wedge t = 0 \rightarrow \neg B$. If $t = 0$ at the start of an iteration, decreasing it would make t negative at the end of the iteration.

   c. Can be false: $p \wedge t > 0 \rightarrow B$. We can have $t > 0$ on loop termination.

   d. Can be false: $p \wedge \neg B \rightarrow t = 0$. Again, $t > 0$ at loop termination is allowed.

e. Must be true: $(p \wedge B \wedge t = t_0) \rightarrow wp(S, t < t_0)$. This guarantees that S reduces t.
f. Must be true: $sp(p \wedge B \wedge t = t_0, S) \rightarrow t < t_0$. This also guarantees that S reduces t.

4. (Possible bound functions for $\{$ ***inv*** $p\}$ $\{$ ***bd*** $t\}$ ***while*** $k \le n$ ***do*** … $k := k+1$ ***od***, where we have $p \rightarrow (n \ge 0 \wedge 0 < C \le k \le n + C$, for constant C (which can be <, =, or > 0).
   a. $(n-k)$: Is decreased by incrementing k, but it can't be a bound function because it can be negative. Since $k \le n + C$, we can subtract $C+k$ from both sides and get $k-(C+k) \le n + C-(C+k)$, which simplifies to $-C \le n-k$.
   b. $n-k+C$: Can be a bound function. Since $k \le n + C$, we know $0 \le n-k+C$, so it's nonnegative, and incrementing k decreases $n-k+C$.
   c. $n+k+C$: Cannot be a bound function because increasing k makes $n+k+C$ larger, not smaller. (It's nonnegative, however: $0 < C \le k \le n+C \Rightarrow 0 < n+C \Rightarrow k < n+k+C$.)
   d. $2 \,\hat{}\, (n+C)/2 \,\hat{}\, k$: Can be a bound function. It's decreased by incrementing k, and it's nonnegative because $0 \le k \le n+C \Rightarrow 2 \,\hat{}\, k \le 2 \,\hat{}\, (n+C) \Rightarrow 2 \,\hat{}\, (n+C)/2 \,\hat{}\, k \ge 1$.

5. (Runtime errors and convergence)
   a. The problem is that $(x/y)^2 - k$ is negative if $x/y = 0$ and $k=1$. Change t by adding 1 so that now, $t \equiv (x/y)^2 - k+1$.[1]
   b. If $p \equiv sqrt(k-1) < x/y$ then $D(p) \Leftrightarrow y \ne 0 \wedge k \ge 1$. Redefine $p \equiv y \ne 0 \wedge k \ge 1 \wedge sqrt(k-1) < x/y$
   c. Change p_0 to $y \ne 0$ so that $p_0 \wedge k = 1 \Rightarrow p$: I.e., $(y \ne 0 \wedge k = 1) \Rightarrow y \ne 0 \wedge k \ge 1 \wedge sqrt(k-1) < x/y$.
   d. We calculate $p_3 \equiv p \wedge t < t_0 \equiv (y \ne 0 \wedge k \ge 1 \wedge sqrt(k-1) < x/y) \wedge ((x/y)^2 - k+1) < t_0$. Since $D(p_3) \Leftrightarrow k \ge 1 \wedge y \ne 0$ and $p_3 \Rightarrow D(p_3)$, p_3 is safe.
   e. $p_2 \equiv wp(k := k+1, p_3) \equiv p_3[k+1/k] \equiv (y \ne 0 \wedge k+1 \ge 1 \wedge sqrt(k+1-1) < x/y) \wedge ((x/y)^2 - (k+1)+1) < t_0$. Since $D(p_2) \Leftrightarrow k \ge 0$ and $p_2 \Rightarrow D(p_2)$, so p_2 is safe.
   f. With $q \equiv sqrt(k-1) < x/y \le sqrt(k)$, We have $D(q) \Leftrightarrow k \ge 1 \wedge y \ne 0$, but q doesn't imply $D(q)$, so we'll redefine q to be the old $(q \wedge D(q))$, which makes the new q safe. The implication $p_4 \Rightarrow q$ does hold, so the predicate logic obligation is met.

      (If you want details for $p_4 \Rightarrow q$, we have $p_4 \equiv p \wedge sqrt(k) \ge x/y$ and $q \equiv sqrt(k-1) < x/y \le sqrt(k) \wedge k \ge 1 \wedge y \ne 0$. (1) Most of q holds because $p_4 \Rightarrow p$, and p includes $k \ge 1$, $y \ne 0$, and $sqrt(k-1) < x/y$. (2) The remainder of q is $x/y \le sqrt(k)$, which is included in p_4.)
   g. The loop test $B \equiv sqrt(k) < x/y$, so $D(B) \Leftrightarrow k \ge 0 \wedge y \ne 0$, and B doesn't imply $D(B)$. This makes $\downarrow B \Leftrightarrow k \ge 0 \wedge y \ne 0 \wedge sqrt(k) < x/y$. We could change the program to use ***while*** $\downarrow B$, but the invariant implies $k \ge 0 \wedge y \ne 0$, so adding it to the loop test is redundant.

---

[1] Just a side mention: We can't use $x/y - sqrt(k)$ as a bound function because it's not always reduced by incrementing k (because of truncation). E.g., $sqrt(4) = sqrt(5) = 2$.