Solution to Homework 6 (Correctness Proofs and Proof Outlines)

Part 1: Complete Formal Proof

1. Below, definitions of p_1, p_2, etc., are given the first time they are used. (Simply listing the definitions was fine too.) The original question parts have been left black.

1.	$\{n \geq 0\}$ k := 0 $\{p_1 \equiv n \geq 0 \wedge k = 0\}$	Assignment
2.	$\{p_1\}$ s := k $\{p_2 \equiv n \geq 0 \wedge k = 0 \wedge s = k\}$	Assignment
3.	$\{n \geq 0\}$ k := 0; s := k $\{p_2\}$	Sequence 1, 2
4.	$\{p_2\}$ r := s $\{p_3 \equiv n \geq 0 \wedge k = 0 \wedge s = k \wedge r = s\}$	Assignment
5.	$p_3 \to p$	Predicate logic
6.	$\{n \geq 0\}$ S_0 $\{p_3\}$	$r_1 \equiv$ Sequence 3, 4
7.	$\{n \geq 0\}$ S_0 $\{p\}$	$r_2 \equiv$ Postcondition weakening 6, 5
8.	$\{p_4 \equiv p[s+r/s]\}$ s := s+r $\{p\}$	Assignment
9.	$\{p_5 \equiv p_4[k+1/k]\}$ k := k+1 $\{p_4\}$	Assignment
10.	$\{p_5\}$ k := k+1; s := s+r $\{p\}$	Sequence 9, 8
11.	$\{p_6 \equiv p_5[r+2*k+1/r]\}$ r := r+2*k+1 $\{p_5\}$	Assignment
12.	$\{p_6\}$ S_1 $\{p\}$	Sequence 11, 10
13.	$p \wedge k < n \to p_6$	$r_3 \equiv$ Predicate logic
14.	$\{p \wedge k < n\}$ S_1 $\{p\}$	$r_4 \equiv$ Precondition Strengthening 13, 12
15.	$\{$**inv** $p\}$ W $\{p \wedge k \geq n\}$ where $W \equiv$ **while** k < n **do** S_1 **od**	while, 14
16.	$p \wedge k \geq n \to s = \text{sum}(n)$	Predicate logic
17.	$\{$**inv** $p\}$ W $\{s = \text{sum}(n)\}$	Postcondition weakening, 14, 15
18.	$\{n \geq 0\}$ S_0; W $\{s = \text{sum}(n)\}$	Sequence, 7, 17

Substitutions:

(Recall $p \equiv 0 \leq k \leq n \wedge s = \text{sum}(k^2) \wedge r = k^2$)

$p_4 \equiv p[s+r/s] \equiv 0 \leq k \leq n \wedge s+r = \text{sum}(k^2) \wedge r = k^2$

$p_5 \equiv p_4[k+1/k] \equiv 0 \leq k+1 \leq n \wedge s+r = \text{sum}((k+1)^2) \wedge r = (k+1)^2$

$p_6 \equiv p_5[r+2*k+1/r] \equiv 0 \leq k+1 \leq n \wedge s+r+2*k+1 = \text{sum}((k+1)^2) \wedge r+2*k+1 = (k+1)^2$

Part 2: Translate Formal Proof into Full Outline

2. (Proof to outline)

$\{n \geq 0\}$ k := 0; $\{p_1\}$ s := 0; $\{p_2\}$ r := 0 $\{p_3\}$

$\{$**inv** $p\}$ **while** k < n **do**

  $\{p \wedge k < n\}$

  $\{p_6\}$ r := r+2*k+1;

  $\{p_5\}$ k := k+1;

  $\{p_4\}$ s := s+r $\{p\}$

od $\{p \wedge k \geq n\}$ $\{s = \text{sum}(n)\}$

Part 3: Expand Minimal Outline

3. (Expand minimal outline)

a. (Use *wp* throughout)

$\{T\}$ $\{(y \geq 0 \to y \geq 0 \to \mathrm{sqrt}(y) = \mathrm{sqrt}(y)) \wedge (y < 0 \to y \geq 0 \to x = \mathrm{sqrt}(y))\}$

if $y \geq 0$ **then**

$\{y \geq 0 \to \mathrm{sqrt}(y) = \mathrm{sqrt}(y)\}$ $x := \mathrm{sqrt}(y)$ $\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$

else

$\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$ **skip** $\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$

fi $\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$

b. (Use *sp* throughout)

$\{T\}$

if $y \geq 0$ **then**

$\{y \geq 0\}$ $x := \mathrm{sqrt}(y)$ $\{y \geq 0 \wedge x = \mathrm{sqrt}(y)\}$

else

$\{y < 0\}$ **skip** $\{y < 0\}$

fi $\{(y \geq 0 \wedge x = \mathrm{sqrt}(y)) \vee y < 0\}$ $\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$

c. (Mix of *wp* and *sp*)

$\{T\}$

if $y \geq 0$ **then**

$\{y \geq 0\}$ $\{y \geq 0 \wedge x = \mathrm{sqrt}(y) = \mathrm{sqrt}(y)\}$ $x := \mathrm{sqrt}(y)$ $\{y \geq 0 \wedge x = \mathrm{sqrt}(y)\}$

else

$\{y < 0\}$ $\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$ **skip** $\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$

fi $\{y \geq 0 \to x = \mathrm{sqrt}(y)\}$

4. (Expand minimal outline) Just to be different, I'm presenting the answer in another format.

$\{b[j] \geq 1\}$	
$x := 1;$ $\{p_1\}$	$p_1 \equiv b[j] \geq 1 \wedge x = 1$
$k := 0;$ $\{p_2\}$	$p_2 \equiv b[j] \geq 1 \wedge x = 1 \wedge k = 0$
$\{$**inv** $p \equiv 1 \leq x = 2\text{^}k \leq b[j]\}$ $\{$**bd** $b[j] - x\}$	
while $2*x \leq b[j]$ **do**	
$\{p \wedge p_3\}$	$p_3 \equiv 2*x \leq b[j] \wedge b[j] - x = t_0$
$\{p_4\}$ $k := k+1$	$p_4 \equiv p_5[k+1/k] \equiv 1 \leq 2*x = 2\text{^}(k+1) \leq b[j] \wedge b[j]-2*x < t_0$
$\{p_5\}$ $x := 2*x$	$p_5 \equiv (p \wedge p_6)[2*x/x] \equiv 1 \leq 2*x = 2\text{^}k \leq b[j] \wedge b[j] - 2*x < t_0$
$\{p \wedge p_6\}$	$p_6 \equiv b[j] - x < t_0$
od $\{p \wedge 2*x > b[j]\}$	
$\{x = 2\text{^}k \leq b[j] < 2\text{^}(k+1)\}$	

Predicate Logic obligations:

$p_2 \to p$, $p \wedge p_3 \to p_4$, and $p \wedge 2*x > b[j] \to x = 2\text{^}k \leq b[j] < 2\text{^}(k+1)$

